

# **ClearPass 6.7**

## **Deployment Guide**



## **Copyright**

© 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

# Contents

---

<b>Copyright .....</b>	<b>2</b>
<b>Contents .....</b>	<b>3</b>
<b>About ClearPass .....</b>	<b>14</b>
About This Guide .....	14
Intended Audience .....	14
About the ClearPass Access Management System .....	15
ClearPass Access Management System Overview .....	15
Key Features .....	16
Advanced Policy Management .....	17
ClearPass Policy Manager Hardware and Virtual Appliances .....	17
ClearPass Specifications .....	18
Accessing the ClearPass Administrative Interface .....	19
Supported Browsers .....	19
Ports Recommended to Be Open .....	20
Specifying the ClearPass Platform License Key Upon Initial Login .....	21
Logging in to the ClearPass Server .....	22
Changing the Administration Password .....	23
Setting Password Policy for Admin Users .....	24
Disabling Admin User Accounts .....	25
ClearPass Menu .....	26
Accessing ClearPass Online Help .....	27
Software Updates .....	27
About Software Updates .....	27
HPE Passport Credentials Considerations .....	27
Maintaining ClearPass Policy Manager Services .....	29
Starting or Stopping ClearPass Services .....	29

---

Summary of the Server Configuration Page .....	30
Subset of CLI for ClearPass Maintenance Tasks .....	31
<b>Preparing the Mobility Controller for ClearPass Policy Manager Integration ...</b>	<b>34</b>
Adding a Mobility Controller to ClearPass Policy Manager .....	34
Defining a New Mobility Controller .....	34
Importing a List of Network Devices .....	36
Generating an Example of Import File XML Format .....	36
Adding a ClearPass/RADIUS Server to the Mobility Controller .....	37
Adding the ClearPass/RADIUS Server to a Server Group .....	41
Configuring an AAA Profile for 802.1X Authentication .....	43
Configuring a Virtual AP Profile .....	48
About Virtual AP Profiles .....	48
Configuring the Virtual AP Profile .....	49
Configuring ClearPass as an RFC 3576 (CoA) Server .....	52
About the CoA Server .....	52
Configuring the ClearPass Server as a CoA Server .....	52
Using the CLI .....	53
Adding an SSID to the Mobility Controller for 802.1X Authentication .....	54
SSID Profile Overview .....	54
Adding an SSID to the Mobility Controller .....	54
<b>Setting Up the ClearPass Hardware and Virtual Appliances ...</b>	<b>60</b>
Setting Up the ClearPass Hardware Appliances .....	60
About the ClearPass Hardware Appliances .....	60
ClearPass C1000 Hardware Appliance .....	61
ClearPass C2000 Hardware Appliance .....	65
ClearPass C3000 Hardware Appliance .....	67
Before Starting the ClearPass Installation .....	70
Configuring the ClearPass Hardware Appliance .....	71

---

---

Activating ClearPass .....	72
Logging in to the ClearPass Hardware Appliance .....	73
Changing the Administration Password .....	74
Powering Off the ClearPass Hardware Appliance .....	75
Resetting the System Passwords to the Factory Defaults .....	75
<b>Using the VMware vSphere Hypervisor Web Client to Install ClearPass on a Virtual Machine .....</b>	<b>76</b>
Introduction .....	77
Virtual Appliance Platforms .....	78
Before Starting the ClearPass Installation .....	78
vSphere Web Client ClearPass Installation Overview .....	79
ClearPass VMware Virtual Appliance Installation Setup .....	79
Adding a Virtual Hard Disk .....	82
Launching the ClearPass Virtual Appliance .....	84
Completing the Virtual Appliance Setup .....	85
Initial Login and Activation of the ClearPass Platform License .....	86
Logging in to the ClearPass Virtual Appliance .....	88
About Software Updates .....	89
Software Updates Page .....	90
Changing the Administration Password .....	93
Powering Off the ClearPass Virtual Appliance .....	93
<b>Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance .....</b>	<b>94</b>
Introduction .....	94
Virtual Appliance Platforms .....	95
Before Starting the ClearPass Installation .....	96
ClearPass Hyper-V Virtual Appliance Installation Summary .....	96
Importing the Virtual Machine .....	97
Adding a Hard Disk to a Virtual Machine .....	101
Launching the ClearPass Virtual Appliance .....	104

---

---

Completing the Virtual Appliance Configuration .....	106
Initial Login and Activation of the ClearPass Platform License .....	107
Logging in to the ClearPass Virtual Appliance .....	108
About Software Updates .....	109
Software Updates Page .....	110
Changing the Administration Password .....	113
Powering Off the ClearPass Virtual Appliance .....	113
<b>Deploying ClearPass Clusters .....</b>	<b>114</b>
ClearPass Cluster Overview .....	114
Introduction .....	114
ClearPass Databases .....	115
Publisher/Subscriber Model .....	116
Network Ports That Must Be Enabled .....	117
Cluster Scaling Limitations .....	118
Cluster Design Considerations .....	118
Cluster Deployment Sizing Guidance .....	118
Publisher Node Guidelines .....	119
Subscriber Node Guidelines .....	120
Providing Sufficient Bandwidth Between Publisher and Subscribers .....	120
Round-Trip Time Considerations for Geographically Distributed Clusters .....	121
Implementing ClearPass Zones for Geographical Regions .....	121
About Large Scale Deployments .....	123
What Is a Large Scale Deployment? .....	123
Design Guidelines .....	124
Examples of Customer Cluster Deployments .....	124
Deploying the Standby Publisher .....	127
Setting Up the Standby Publisher .....	127
About the Fail-Over Process .....	128

---

---

Mitigation Strategies .....	128
Virtual IP Address Considerations .....	129
Functions Lost When the Publisher Is Down .....	129
Adding a Subscriber Node to the Publisher .....	129
Introduction .....	129
Using the WebUI to Add a Subscriber Node .....	130
Using the CLI to Create a Subscriber Node .....	133
Rejoining a Down Node to the Cluster .....	133
Introduction .....	133
Removing a Subscriber Node from the Cluster .....	134
Rejoining a Disabled Node Back Into the Cluster .....	135
Deploying ClearPass Insight in a Cluster .....	136
Introduction .....	136
ClearPass Insight Placement Considerations .....	136
When a ClearPass Insight-Enabled Node Is Down .....	137
Enabling ClearPass Insight .....	137
Configuring Cluster File-Backup Servers .....	137
Adding Cluster File-Backup Servers .....	138
Backing Up Configuration and Access Tracker Log Information .....	139
Cluster CLI Commands .....	140
cluster drop-subscriber .....	140
cluster list .....	141
cluster make-publisher .....	141
cluster make-subscriber .....	141
cluster reset-database .....	142
cluster set-cluster-passwd .....	142
cluster sync-cluster-passwd .....	143

---

## **Preparing for Active Directory Authentication ..... 144**

Joining a ClearPass Server to an Active Directory Domain .....	144
Introduction .....	144
Synchronizing the Cluster Date and Time with the NTP Server .....	145
Joining an Active Directory Domain .....	150
About the Authentication Source and the Authorization Process .....	155
Manually Configuring Active Directory Password Servers .....	155
Disassociating a ClearPass Server From an Active Directory Domain .....	156
Adding Active Directory as an Authentication Source to ClearPass .....	157
About Authorization .....	157
User Objects .....	157
About the Bind Operation .....	158
Adding Active Directory as an Authentication Source .....	158
Obtaining and Installing a Signed Certificate From Active Directory .....	164
About Certificates in ClearPass Deployments .....	164
Tasks to Obtain a Signed Certificate from Active Directory .....	165
Creating a Certificate Signing Request .....	165
Importing the Root CA Files to the Certificate Trust List .....	167
Obtaining a Signed Certificate from Active Directory .....	169
Importing a Server Certificate into ClearPass .....	171
Manually Testing Login Credentials Against Active Directory .....	173

## **Preparing for 802.1X Wireless Authentication with Active Directory ..... 174**

About 802.1X Authentication .....	174
Introducing 802.1X .....	174
802.1X Authentication Components .....	174
What Is AAA? .....	176
Authentication .....	176
Authorization .....	176

---

Accounting .....	176
Configuring 802.1X Wireless Authentication with Active Directory .....	176
Authenticating Against Active Directory .....	177
About the 802.1X Wireless Service .....	177
Creating the 802.1X Wireless Service .....	178
Deleting a ClearPass Policy Manager Service .....	182
Walking Through an 802.1X Authentication Scenario .....	183
802.1X Wireless Authentication Traffic Flow .....	183
Walking Through the 802.1X Authentication Process .....	183
802.1X Wired Authentication Traffic Flow .....	184
Troubleshooting 802.1X Configuration Issues .....	184
Active Directory Authentication Source Configuration Issues .....	184
Mobility Controller Configuration Issues .....	184
<b>Integrating the ArubaOS Switch with ClearPass .....</b>	<b>186</b>
About the ArubaOS Switch .....	186
Overview .....	186
Unified Management with ClearPass Policy Manager .....	187
Initial ArubaOS Switch Configuration .....	187
Configuring Administrator Credentials .....	187
Configuring the IP Address of the Out-of-Band Management Port .....	187
Configuring SNMPv3 .....	188
Configuring a ClearPass/RADIUS Server on the Switch .....	189
Defining the ArubaOS Switch in ClearPass .....	190
Setting Up RADIUS Authentication, Authorization, and Accounting .....	191
About AAA Services .....	191
About the RADIUS Protocol .....	192
About the TACACS+ Protocol .....	192
Setting Up RADIUS Accounting .....	193

---

---

Additional Configuration Considerations .....	195
<b>Authenticating Users to the ArubaOS Switch .....</b>	<b>196</b>
Why Use ClearPass to Perform Authentication and Authorization for the ArubaOS Switch? .....	196
What are the Supported Protocols for ArubaOS Switch Management Authentication and Authorization? .....	196
What Are the Pros and Cons of TACACS vs RADIUS for Authentication and Authorization? .....	196
<b>Switch Management Using TACACS+ .....</b>	<b>196</b>
Overview .....	196
Setting Up Switch Management Using TACACS+ .....	197
Creating Enforcement Profiles to Provide Manager Access and Command Control to the ArubaOS Switch .....	198
Creating an Enforcement Policy to Define Access to the Switch .....	205
Creating a Service to Support TACACS+ Authentication Requests from the Switch .....	207
Setting Up the Switch for Command Authorization Using TACACS+ .....	210
Setting Up Enforcement Profiles in ClearPass to Support TACACS+ Command Authorization Requests from the Switch .....	210
<b>Switch Management Using RADIUS .....</b>	<b>214</b>
Setting Up Switch Management Using RADIUS .....	214
Using RADIUS-Based Authentication and Command Authorization .....	216
Creating Enforcement Profiles to Provide Manager Access and Command Authorization to the ArubaOS Switch .....	216
Creating an Enforcement Policy to Define Access to the Switch .....	221
Setting Up a Service in ClearPass to Support RADIUS Authentication Requests From the Switch .....	224
<b>OnGuard Authentication Configuration .....</b>	<b>227</b>
Overview .....	227
OnGuard Configuration Workflow .....	228
ClearPass Configuration .....	228
<b>Monitoring and Troubleshooting .....</b>	<b>234</b>
Monitoring Active 802.1X Sessions .....	235
Monitoring RADIUS Messages .....	235

---

---

**Integrating ClearPass with a Cisco Switch .....** **238**

Introduction .....	238
Cisco Switch Configuration for ClearPass .....	238
Introduction .....	239
VLAN Numbers .....	239
Configuring the Cisco Switch .....	239
Supplemental Configuration Information .....	241
802.1X Service Setup .....	242
Introduction .....	242
Adding an Enforcement Profile for VLAN 999 .....	242
Cisco Downloadable ACL (dACL) Setup .....	244
Introduction .....	244
Adding a Cisco dACL Enforcement Profile .....	245
Adding a dACL Enforcement Policy .....	245
Creating the 802.1X Wired Service .....	247

**Mobility Access Switch Configuration for 802.1X Authentication .....** **250**

Mobility Access Switch Configuration for 802.1X Wired Authentication .....	250
About Defining Wired 802.1X Authentication .....	250
Configuring Authentication with a RADIUS Server .....	251
Authentication Terminated on the Mobility Access Switch .....	252
Configuring Access Control Lists .....	253
CLI-Based Configuration for Mobility Access Switch 802.1X Authentication .....	254
Termination Options .....	254
Configuring a Server Rule Using the CLI .....	256
Setting Variables for LDAP Servers .....	256
Configuring Certificates with Authentication Termination .....	256
Configuring 802.1X Authentication with Machine Authentication .....	257
About Machine Authentication .....	257

---

Enabling the Enforce Machine Authentication Option .....	257
Role Assignment with Machine Authentication Enabled .....	258
VLAN Assignments .....	259
Authentication with an 802.1x RADIUS Server .....	260
Examples of Common 802.1X Configuration Tasks Via the CLI .....	261
<b>Preparing ClearPass for LDAP and SQL Authentication Sources .....</b>	<b>264</b>
<b>LDAP Authentication Source Configuration .....</b>	<b>264</b>
Configuring Generic LDAP Authentication Sources .....	264
<b>SQL Authentication Source Configuration .....</b>	<b>269</b>
Configuring a Generic SQL Authentication Source .....	269
Defining a Filter Query .....	273
<b>802.1X EAP-PEAP Reference .....</b>	<b>276</b>
A Tour of the EAP-PEAP-MSCHAPv2 Ladder .....	276
About EAP-PEAP MSCHAPv2 .....	276
EAP-PEAP MSCHAPv2 Handshake Exchange Summary .....	276
<b>Using the ClearPass Configuration API .....</b>	<b>284</b>
<b>ClearPass Configuration API Overview .....</b>	<b>284</b>
Introduction .....	284
Admin Accounts for API Access .....	284
XML Data Structure .....	285
Filter Elements .....	286
Advanced Match Operations .....	286
Setting Up Bulk Access for Endpoints and Guest Accounts .....	287
<b>ClearPass Configuration API Methods .....</b>	<b>289</b>
Introduction .....	289
Authentication Credentials .....	289
Entity Names Supported .....	290
NameList .....	291

---

---

Reorder .....	292
Status Change .....	293
<a href="#">ClearPass Configuration API Examples</a> .....	294
Introduction .....	294
Using the Contains Match Operator .....	294
Retrieving a Guest User Value .....	294
Retrieving a Local User Value .....	295
Adding a Guest User Value .....	296
Updating a Guest User Value .....	296
Removing a Guest User .....	297
<a href="#">API Error Handling</a> .....	299
When There Is an Error During a Request .....	299
InvalidFetchCriteria Example .....	299
<a href="#">About the API Explorer</a> .....	300

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

This chapter includes the following information:

- [About This Guide](#)
- [About the ClearPass Access Management System](#)
- [Maintaining ClearPass Policy Manager Services](#)

## **About This Guide**

Welcome to the *ClearPass 6.7 Deployment Guide*.

The *ClearPass 6.7 Deployment Guide* is intended to assist field System Engineers and network administrators, as well as customers and partners, in deploying ClearPass Policy Manager.

This 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.

The *ClearPass 6.7 Deployment Guide* includes the following information:

- [Chapter 1](#): An overview of the ClearPass Policy Manager Access Management System.
- [Chapter 2](#): Install and configure ClearPass hardware and virtual appliances.
- [Chapter 3](#): Prepare the Mobility Controller for integration with ClearPass Policy Manager.
- [Chapter 4](#): Integrate ClearPass Policy Manager with Microsoft Active Directory.
- [Chapter 5](#): Set up 802.1X wireless authentication with Active Directory.
- [Chapter 6](#): Design and deploy ClearPass clusters.
- [Chapter 7](#): Integrating the ArubaOS switch with ClearPass
- [Chapter 8](#): Integrating the Cisco Switch with ClearPass
- [Chapter 9](#): Configure the Mobility Access Switch for 802.1X wired authentication
- [Chapter 10](#): Prepare ClearPass for LDAP and SQL authentication.
- [Appendix A](#): Describes how a typical 802.1X EAP-PEAP authentication session flows when using ClearPass as the authentication server with Microsoft Active Directory as the back-end user identity repository.
- [Appendix B](#): Use the ClearPass Configuration API to configure or modify the entities in ClearPass without logging into the Admin user interface. Information about how to access the entire set of APIs available through ClearPass is also provided.

## **Intended Audience**

The intended audience for the *ClearPass Deployment Guide* includes customers, partners, and field System Engineers.

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

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

- AAA technologies (RADIUS, TACACS, 802.1X, MAC address authentication, and Web authentication)
- Layer-2 and Layer-3 networking
- Microsoft Active Directory
- Switch technologies: ArubaOS switch, Cisco switches, Aruba Mobility Access Switch



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

## About the ClearPass Access Management System

This section contains the following information:

- [ClearPass Access Management System Overview](#)
- [Key Features](#)
- [Advanced Policy Management](#)
- [ClearPass Policy Manager Hardware and Virtual Appliances](#)
- [ClearPass Specifications](#)

### ClearPass Access Management System Overview

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

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

### Role-Based and Device-Based Access

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

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

### Self-Service Capabilities

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

### Leveraging Contextual Data

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

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

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

## Third-Party Security and IT Systems

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

## Key Features

ClearPass's key features are as follows:

- 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) for BYOD.
- 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, which allows seamless single sign-on (SSO) to cloud or on-premise applications.
- SAML 2.0 Service Provider, which allows 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 single sign-on (SSO) via OAuth 2.0
- Facebook, Twitter, LinkedIn, Azure Active Directory and Office 365, Google G Suite, 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

## Advanced Policy Management

ClearPass advanced policy management support includes:

- **Employee access**

ClearPass Policy Manager 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, 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.

- **Built-in device profiling**

ClearPass provides a built-in 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 health-check capabilities ensure compliance and network safeguards before devices connect.

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

## ClearPass Policy Manager Hardware and Virtual Appliances

ClearPass Policy Manager is available as a hardware or a virtual appliance. To increase scalability and redundancy, you can deploy virtual appliances, as well as the hardware appliances, within a cluster.

- For hardware and virtual appliance installation and deployment procedures, see [Setting Up the ClearPass Hardware and Virtual Appliances](#).

Virtual appliances are supported on the following platforms:

- VMware ESX and ESXi
  - For installation and deployment procedures, see [Using the VMware vSphere Hypervisor Web Client to Install ClearPass on a Virtual Machine](#).
- Microsoft Hyper-V
  - For installation and deployment procedures, see [Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance](#).

## ClearPass Specifications

### Hardware and Virtual Appliances

ClearPass is available as hardware or as a virtual appliance. Virtual appliances are supported on VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V, and Amazon EC2.

- VMware ESXi 5.5 up to 6.5 Update 1
- Microsoft Hyper-V Server 2012 R2/2016, and Windows Server 2012 R2 with Hyper-V
- Amazon AWS (EC2)

### ClearPass Platform

- Deployment templates for any network type, identity store, and endpoint
- 802.1X, MAC authentication and captive portal support
- ClearPass OnConnect for SNMP-based enforcement on wired switches
- Advanced reporting, analytics and troubleshooting tools
- Interactive policy simulation and monitor mode utilities
- Multiple device registration portals—Guest, Aruba AirGroup, BYOD (bring your own device), and unmanaged devices
- Admin/Operator access security via CAC (Common Access Card) and TLS (Transport Layer Security) certificates

### 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 .02
- Microsoft NAP and 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)

## **IPv6 Support**

- Web and CLI based management
- IPv6 addressed authentication & authorization servers
- IPv6 accounting proxy
- IPv6 addressed endpoint context servers
- Syslog, DNS, NTP, IPsec IPv6 targets
- IPv6 Virtual IP for high availability
- HTTP Proxy
- Ingress Event Engine Syslog sources

## **Profiling Methods**

- Active: Nmap, WMI, SSH, SNMP
- Passive: MAC OUI, DHCP, TCP, Netflow v5/v10, IPFIX, sFLOW, 'SPAN' Port, HTTP User-Agent, IF-MAP
- Integrated and Third-Party: Onboard, OnGuard, ArubaOS, EMM/MDM, Rapid7, Cisco device sensor

# **Accessing the ClearPass Administrative Interface**

This section contains the following information:

- [Supported Browsers](#)
- [Ports Recommended to Be Open](#)
- [Specifying the ClearPass Platform License Key Upon Initial Login](#)
- [Logging in to the ClearPass Server](#)
- [Changing the Administration Password](#)
- [Setting Password Policy for Admin Users](#)
- [Disabling Admin User Accounts](#)
- [ClearPass Menu](#)
- [Accessing ClearPass Online Help](#)

## **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.

## **Ports Recommended to Be Open**

[Table 1](#) lists all the ports that are required by ClearPass Policy Manager to properly operate within your environment, as well as the ports that are strongly recommended having them open.

**Table 1:** *Required and Recommended Open Ports*

Port	Protocol	Service/Application Use
<b>Ports Required to Be Open</b>		
22	TCP	Secure Shell (SSH)
80	TCP	HTTP
123	UDP	Network Time Protocol (NTP)
443	TCP	HTTPS
1645	UDP	RADIUS (Auth)
1646	UDP	RADIUS (Acct)
1812	UDP	RADIUS (Auth)
1813	UDP	RADIUS (Acct)
5432	TCP	Database System
<b>Ports Recommended to Be Open</b>		
49	TCP	TACACS+
67	UDP	DHCP Snooper
161	UDP	SNMP

Port	Protocol	Service/Application Use
162	UDP	SNMP
6658	TCP	Agent Controller

## Specifying the ClearPass Platform License Key Upon Initial Login

Upon initial login to a ClearPass 6.7 server and later, you are prompted to enter the ClearPass Platform License Key. The ClearPass 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.



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 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 or later server.

The ClearPass End-User Software License Agreement dialog appears.

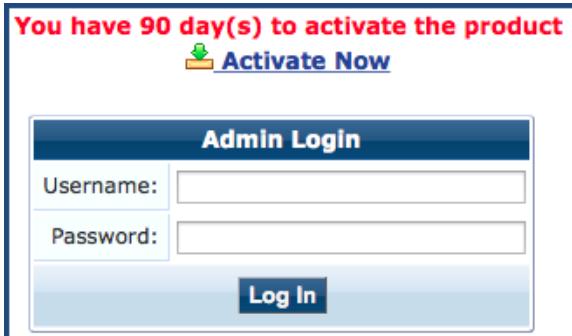
The *Select Application* field is preset to **ClearPass Platform**.

**Figure 1** Entering the ClearPass Platform License Key

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 2** Activating the ClearPass Node



6. To activate the ClearPass Platform License on this appliance, click the **Activate Now** link.

The **Activate License** dialog opens:

**Figure 3** Activating the ClearPass Platform License



7. If the ClearPass server is connected to the Internet, click the **Activate Now** button.

You receive the message, "*Product has been successfully activated*" and the **Admin Login** dialog is displayed.

## Logging in to the ClearPass Server

The password you should 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. Enter the password that was set up during the installation process (see [Configuring the ClearPass Hardware Appliance on page 71](#)).
  - 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 appropriate password.
- Click **Log In**.
- The **ClearPass Policy Manager Landing Page** opens.

## Changing the Administration Password

The recommended next task is to change the administration password for the newly-active ClearPass server.

To change the administration password:

- In ClearPass, navigate to **Administration > Users and Privileges > Admin Users**.  
The **Admin Users** page opens.

**Figure 4** Admin Users Page

#	User ID	Name	Privilege Level	Status
1.	<input checked="" type="checkbox"/> admin	Super Admin	Super Administrator	Enabled
2.	<input type="checkbox"/> apiaadmin	API Admin	API Administrator	Enabled

- Select the Admin user you want to modify.

The **Edit Admin User** dialog opens.

**Figure 5** Changing the Administration Password

User ID:	admin
Name:	Super Admin
Password:	••••••••••
Verify Password:	••••••••••
Enable User:	<input checked="" type="checkbox"/> (Check to enable user)
Privilege Level	Super Administrator
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

- Change the administration password, then click **Save**.

Specify the **Edit Admin User** parameters as described in [Table 2](#), then click **Save**.

**Table 2:** Edit Admin User Parameters

Parameter	Action/Description
User ID	Specify a user ID for this administrator.

Parameter	Action/Description
Name	Specify the name for the admin user.
Password/ Verify Password	Specify a password for the local user, then verify the password.
Enable User	You must enable this check box to enable the admin user account (it is enabled by default). Otherwise, the admin user account is disabled.
Privilege Level	<p>Indicates the admin user privilege level set for this admin user:</p> <ul style="list-style-type: none"> <li>● Super Administrator</li> <li>● Aruba User Role Download</li> <li>● API Administrator</li> <li>● Help Desk</li> <li>● Network Administrator</li> <li>● Read-only Administrator</li> <li>● Receptionist</li> </ul>

## 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 6** Admin Users > Setting Password Policy

Account Settings	
<b>Password Policy</b>	
Minimum Length:	<input type="text" value="6"/>
Complexity:	<input type="text" value="No password complexity requirement"/>
Disallowable Characters:	<input type="text"/>
Disallowable Words (CSV):	<input type="text"/>
Additional checks:	<input type="checkbox"/> May not contain User ID or its characters in reversed order <input type="checkbox"/> May not contain repeated character four or more times consecutively
Expiry Days:	<input type="text" value="0"/>
<b>Note:</b> Password characters validation will take effect for users created or modified after changes are saved. Other settings will be applied to all users.	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

3. Specify the **Password Policy** parameters as described in [Table 3](#), then click **Save**:

**Table 3:** Password Policy Parameters

Parameter	Action/Description
Minimum Length	Specify the minimum length required for the password.
Complexity	Select the complexity setting from the <b>Complexity</b> drop-down list. The complexity settings must be one of the following: <ul style="list-style-type: none"><li>● No password complexity requirement</li><li>● At least one uppercase and one lowercase letter</li><li>● At least one digit</li><li>● At least one letter and one digit</li><li>● At least one of each: uppercase letter, lowercase letter, digit</li><li>● At least one symbol</li><li>● At least one of each: uppercase letter, lowercase letter, digit, and symbol</li></ul>
Disallowed Characters	Specify the characters not to be allowed in the password.
Disallowed Words (CSV)	Specify the words not to be allowed in the password.
Additional Checks	Select any additional checks, if required. The options are: <ul style="list-style-type: none"><li>● May not contain User ID or its characters in reversed order.</li><li>● May not contain repeated character four or more times consecutively.</li></ul>
Expiry Days	Set the password expiry time for the local users. The allowed range is <b>0</b> to <b>500</b> days. The default value is <b>0</b> . <b>NOTE:</b> If the value is set to <b>0</b> , 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.

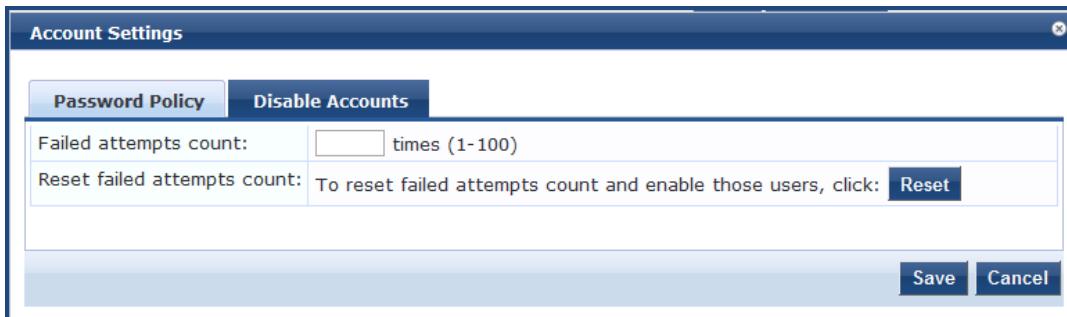
## Disabling Admin User Accounts

- The **Disable Account** check occurs every day at midnight.
- Other Local User configuration settings are applied to all local users.

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 7** Admin Users > Disable Accounts Dialog



4. Specify the **Disable Accounts** parameters as described in [Table 4](#), then click **Save**.

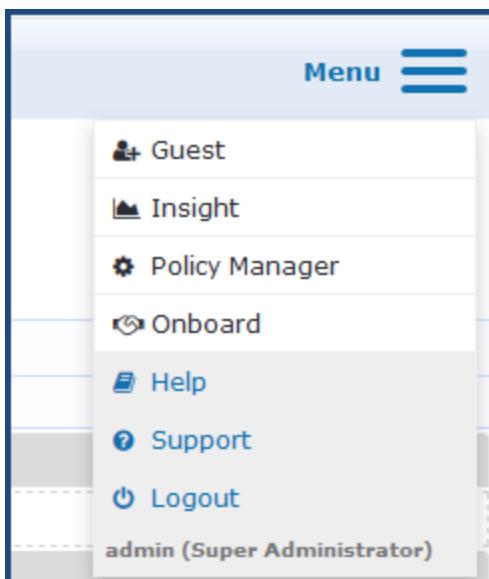
**Table 4:** Admin Users > Disable Accounts Parameters

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

## ClearPass Menu

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

**Figure 8** 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

## Accessing ClearPass Online Help

The *ClearPass Policy Manager User Guide* is incorporated into the Online Help system. All Policy Manager features include context-sensitive help.

To access context-sensitive help, click the **Help** link at the top right-hand corner of any ClearPass page.

## Software Updates

This section contains the following information:

- [About Software Updates](#)
- [HPE Passport Credentials Considerations](#)

### About Software Updates

ClearPass 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 Parameters** 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 [Cluster-Wide Parameters General page](#) for more information).

You can also:

- Reinstall a patch in the event the previous installation attempt fails.
- Uninstall a skin.

### HPE Passport Credentials Considerations

The HPE Passport account credentials that are associated with a customers' ClearPass licenses are used to validate entitlement.

HPE recommends that customers use a generic HPE Passport account (for example, *clearpass@customerX.com* or *CustomerXClearPass*) to avoid any future issues should an individual employee leave the business and the HPE Passport account is closed or the password is forgotten.

Legacy ClearPass licenses and their associated Subscription ID(s) should be moved to this account first before initiating the license conversions. This ensures that the legacy Subscription ID information is properly mapped to the HPE Passport account credentials.

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

**Figure 9** Entering the HPE Passport Credentials for Live Updates

The screenshot shows the 'Software Updates' page under 'Agents and Software Updates'. At the top, there's a 'HPE Passport Credentials' section with fields for 'Username' (HPEpassport@hpe.com) and 'Password' (redacted). A 'Save' button is to the right. Below this is a 'Posture & Profile Data Updates' table:

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
Posture Signature Updates*	1.49236	2017/11/01 13:30:05	Online	2017/11/01 22:00:03	Updated 1 day ago
Windows Hotfixes Updates*	1.2181	2017/10/31 16:50:27	Online	2017/11/01 22:00:05	Updated 1 day ago
Endpoint Profile Fingerprints*	2.545	2017/10/24 11:15:29	File	2017/11/01 15:06:21	Updated 1 day ago

A 'Import Updates' button is at the bottom of this section. Below it is a note: '\* Automatic download and install is disabled. To manually import Posture & Profile Data Updates, refer to Help for this page.' The 'Firmware & Patch Updates' section follows, with a table:

Update Type	Name	Version	Size (MB)	Update Released	Last Checked	Status	Delete
Patch	6.7.0.100772*	-	0.0040	2017/11/15	2017/11/02 16:10:22	Download	-
Patch	ClearPass OnGuard Engine 1.0 Update 1†‡	1.0.0.101255	62.7049	2017/10/30	2017/11/02 16:10:22	Installed	-
Guest Skin	Fidelity Investments Skin	0.1.6-0	0.6084	2013/09/09	2017/11/02 16:10:22	Download	-

A 'Import Updates' button is at the bottom of this section. Below it are small notes: \* Needs Restart, † Restarts Administration UI, ‡ Last Installed, available for Re-Install. At the very bottom is a 'Check Status Now' button.

2. If the ClearPassPolicy Manager has Internet access, enter your HPE Passport Credentials, then click **Save**.

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.

After successfully applying the HPE Passport Credentials, you will see a message indicating that the HPE Passport Credentials were updated successfully and ClearPass is processing updates from the ClearPass Webservice.

Note that *Posture & Profile Data Updates* are downloaded and installed when configured accordingly, while *Firmware & Patch Updates* are display only.

# Maintaining ClearPass Policy Manager Services

This section contains the following information:

- [Starting or Stopping ClearPass Services](#)
- [Summary of the Server Configuration Page](#)
- [Subset of CLI for ClearPass Maintenance Tasks](#)

## Starting or Stopping ClearPass Services

From the **Services Control** page, you can view the status of a service (that is, see whether a service is running or not), and stop or start Policy Manager services, including any Active Directory domains to which the current server is now joined.

To access the **Services Control** page:

1. In ClearPass, navigate to **Administration > Server Manager > Server Configuration**.  
The **Server Configuration** page opens.
2. Click the row that lists the ClearPass server of interest.  
The **Server Configuration** screen for the selected ClearPass server opens.

**Figure 10** ClearPass Server Configuration Page for Selected Server

The screenshot shows the 'Server Configuration' page for a server named '51.120'. The 'Services Control' tab is active. The page includes sections for basic server info (Hostname, FQDN, Policy Manager Zone), performance monitoring (Enable Performance Monitoring Display), insight settings (Enable Insight), and network ports (Management Port, Data/External Port, DNS Settings). The 'AD Domains' section indicates the server is not part of any domain and provides a 'Join AD Domain' button.

3. Select the **Services Control** tab.

The **Services Control** page opens.

**Figure 11** Server Configuration > Services Control Page

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Service Name		Status	Action		
1.	AirGroup notification service	Running	Stop		
2.	Async DB write service	Running	Stop		
3.	Async network services	Running	Stop		
4.	ClearPass IPsec service	Running	Stop		
5.	DB change notification server	Running	Stop		
6.	DB replication service	Running	Stop		
7.	Extensions service	Running	Stop		
8.	Ingress logger service	Stopped	Start		
9.	Ingress logrepo service	Stopped	Start		
10.	Micros Fidelio FIAS	Running	Stop		
11.	Multi-master cache	Running	Stop		
12.	Policy server	Running	Stop		
13.	Radius server	Running	Stop		
14.	Stats aggregation service	Running	Stop		
15.	Stats collection service	Running	Stop		
16.	System auxiliary services	Running	Stop		
17.	System monitor service	Running	Stop		
18.	Tacacs server	Running	Stop		
19.	Virtual IP service	Stopped	Start		

[Back to Server Configuration](#) Save Cancel



You will notice that the Virtual IP service is the only service that is not running. It's normal for the Virtual IP service to be stopped when it is not being used.

From the **Services Control** page, you can:

- View the status of all the services: Running or Stopped.
- Stop or start ClearPass services, including any Active Directory domains that the server joins.
- If a service is stopped, use its **Start** button to restart it.

### Starting Services from the Command Line

- You can also start an individual service from the command line:

```
service start <service_name>
```

- You can start all the services from the command line:

```
service start all
```

## Summary of the Server Configuration Page

The **Server Configuration** page provides many options.

[Table 5](#) describes each of the top-level server configuration options that are available. For details, refer to the "Server Configuration" section in the "Administration" chapter of the *ClearPass Policy Manager User Guide*.

**Table 5:** Description of the Server Configuration Page

Tab	Description	Comments
System	Displays server identity and connection parameters. The configurations for the management port and the data port are also displayed.	This tab also provides parameters to allow you to enable Insight and specify the Insight master, enable OnConnect, and enable ingress events processing.

Tab	Description	Comments
<b>Services Control</b>	You can view the status of a Policy Manager service (that is, see whether a service is running or not), and stop or start services.	
<b>Service Parameters</b>	This option allows you to change the system parameters for all services.	The options on this page vary based on the service selected.
<b>System Monitoring</b>	This option allows you to configure SNMP parameters, ensuring that external MIB browsers can browse the system-level MIB objects exposed by the Policy Manager appliance.	The options on this page vary based on the SNMP version that you select.
<b>Network</b>	<p>Use the Network page to:</p> <ul style="list-style-type: none"> <li>• Configure Application Access Control—allow or deny access to network resources.</li> <li>• Add SSH Public Keys</li> <li>• Create generic routing encapsulation (GRE) tunnels</li> <li>• Create IPsec tunnels</li> <li>• Create VLANs related to guest users.</li> </ul>	<ul style="list-style-type: none"> <li>• A GRE tunnel creates a virtual point-to-point link between controllers over a standard IP network or the Internet.</li> <li>• To create VLANs, your network infrastructure must support tagged 802.1Q packets on the physical interface selected.</li> </ul>
<b>FIPS</b>	Enables ClearPass to operate in Federal Information Processing Standard mode.	<p>For most users, this tab should be ignored.</p> <p><b>NOTE:</b> Enabling FIPS mode resets the database.</p>

## Subset of CLI for ClearPass Maintenance Tasks

The CLI provides a way to manage and configure Policy Manager information.

You can access the CLI from the console using the serial port on the ClearPass appliance hardware, or remotely using SSH, or use the VMware vSphere, Microsoft Hyper-V, or KVM console to run the virtual appliance.

```
*****
* Policy Manager CLI v6.7(0), Copyright © 2017, Aruba Networks, an HPE Company
*
* Software Version : 6.7.0 062080
*****
Logged in as group Local Administrator
[appadmin@company.com]#
```

## CLI Task Examples

### View the Policy Manager Data and Management Port IP Address and DNS Configuration

```
[appadmin]#show ip
```

### Reconfigure DNS or Add a New DNS

```
[appadmin]#configure dns <primary> [secondary] [tertiary]
```

## Reconfigure or Add Management and Data Ports

```
[appadmin]#configure ip <mgmt | data > <ipadd> netmask <netmask address> gateway <gateway address>
```

Parameter	Description
ip <mgmt  data> <ip address>	<ul style="list-style-type: none"><li>Network interface type: <i>mgmt</i> (management) or <i>data</i></li><li>Server IP address</li></ul>
netmask <netmask address>	Netmask to be applied to the network interface and server IP addresss
gateway <gateway address>	Gateway IP address

## Configure the Date

Configuring the time and time zone is optional.

```
[appadmin]#configure date -d <date> [-t <time>] [-z <timezone>]
```

## Configure the Host Name for the Node

```
[appadmin]##configure hostname <hostname>
```

## Join the ClearPass Policy Manager Appliance to the Active Directory Domain

If you are using Active Directory to authenticate users, be sure to join the ClearPass Policy Manager appliance to the Active Directory domain.

```
[appadmin]#ad netjoin <domain-controller.domain-name> [domain NetBIOS_name]
```

Flag/Parameter	Description
<domain-controller.domain-name>	Required. This is the name of the host to be joined to the domain. <b>NOTE:</b> Use the Fully Qualified Domain Name.
[domain NetBIOS name]	Optional.



# Preparing the Mobility Controller for ClearPass Policy Manager Integration

This chapter describes how to prepare the Mobility Controller in order to integrate with ClearPass Policy Manager.

This chapter includes the following information:

- [Adding a Mobility Controller to ClearPass Policy Manager](#)
- [Adding a ClearPass/RADIUS Server to the Mobility Controller](#)
- [Adding the ClearPass/RADIUS Server to a Server Group](#)
- [Configuring an AAA Profile for 802.1X Authentication](#)
- [Configuring a Virtual AP Profile](#)
- [Configuring ClearPass as an RFC 3576 \(CoA\) Server](#)
- [Adding an SSID to the Mobility Controller for 802.1X Authentication](#)

## Adding a Mobility Controller to ClearPass Policy Manager

This section describes how to add a mobility controller to ClearPass Policy Manager.

This section contains the following information:

- [Defining a New Mobility Controller](#)
- [Importing a List of Network Devices](#)
- [Generating an Example of Import File XML Format](#)

### Defining a New Mobility Controller

The mobility controller is responsible for managing access to the Wireless LAN.



You can use this procedure to add any network device from any vendor that supports RADIUS or TACACS+ to ClearPass Policy Manager.

To define a new mobility controller in ClearPass:

1. In ClearPass Policy Manager, navigate to **Configuration > Network > Devices**.  
The **Network Devices** screen opens:

**Figure 12** Network Devices Screen

The screenshot shows the 'Network Devices' screen in ClearPass Policy Manager. At the top, there's a navigation bar: Configuration > Network > Devices. Below the navigation is a search bar labeled 'Filter: Name' with a dropdown menu set to 'contains'. There are also 'Go' and 'Clear Filter' buttons. To the right of the search bar are three icons: 'Add' (green plus), 'Import' (blue folder), and 'Export All' (orange folder). Further to the right is a link to 'Discovered Devices'. On the far right, there's a button to 'Show 10 records'. The main area is a table with columns: '#', 'Name ▲', 'IP or Subnet Address', and 'Description'. The table lists three entries: '1. 10.' (IP 10.0.0.1), '2. 10.' (IP 10.0.0.2), and '3. amgController' (IP 10.0.0.3, Description 'public'). The row for 'amgController' is highlighted with a yellow background. At the bottom left, it says 'Showing 1-3 of 3'. At the bottom right, there are 'Copy', 'Export', and 'Delete' buttons.

- Click the **Add** link.

The **Add Device** page opens:

You can also import a list of devices from a file. For details, see [Importing a List of Network Devices](#).

**Figure 13** Add Device Page > Device Tab

The screenshot shows the 'Add Device' dialog box with the 'Device' tab selected. The 'Attributes' section contains the following fields:

- Name: [Text input field]
- IP or Subnet Address: [Text input field] (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)
- Description: [Text area]
- RADIUS Shared Secret: [Text input field] Verify: [Text input field]
- TACACS+ Shared Secret: [Text input field] Verify: [Text input field]
- Vendor Name: Aruba [Dropdown menu]
- Enable RADIUS CoA:  RADIUS CoA Port: 3799 [Text input field]

At the bottom right are 'Add' and 'Cancel' buttons.

- Populate the **Network Device** parameters as described in [Table 6](#).

**Table 6:** Defining a Mobility Controller

Parameter	Action/Description
Name	Enter the name of the Mobility Controller.
IP or Subnet Address	Enter the IP address or subnet address of the Mobility Controller.
Description	Enter a description of the device (recommended).
RADIUS Shared Secret	Specify the RADIUS Shared Secret for the current ClearPass Policy Manager server. <b>NOTE:</b> Make sure that the value of the <b>Key</b> parameter for the RADIUS server configured on the mobility controller is identical to the RADIUS Shared Secret you specify here for the current Policy Manager server (see <a href="#">Table 7</a> ).
TACACS Shared Secret	If you're adding a device because you want ClearPass to manage access to that device with TACACS+, specify the TACACS+ Shared Secret.
Vendor Name	From the drop-down, select the manufacturer of the controller.
Enable RADIUS CoA	To enable RADIUS-initiated Change of Authorization (CoA) on the mobility controller, select the check box for this parameter. This parameter is enabled by default.

Parameter	Action/Description
RADIUS CoA Port	If RADIUS CoA is enabled, this specifies the default port <b>3799</b> . Change this value only if you defined a custom port on the mobility controller. For related information, see <a href="#">Configuring ClearPass as an RFC 3576 (CoA) Server</a> .

4. Click **Add**.

You return to the **Network Devices** page. The new mobility controller is now present in the list of network devices.

## Importing a List of Network Devices

To import a list of network devices from a file:



The import file must be in XML format. See the next section for an example of the import file XML format.

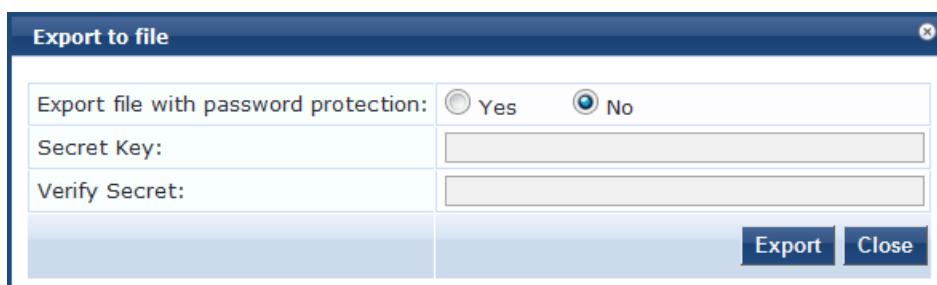
1. In ClearPass Policy Manager, navigate to **Configuration > Network > Devices**.  
The **Network Devices** page opens.
2. From the **Network Devices** page, click **Import**, then click **Import from file**.  
The **Import from File** dialog opens.
2. To browse to the file, click **Browse**.
3. Enter the shared secret if required, then click **Import**.  
The list of network devices is imported into ClearPass.

## Generating an Example of Import File XML Format

To generate an example of the import file XML format:

1. From the **Network Devices** dialog, click the **Add** link.  
The **Add Device** dialog opens.
2. In the **Device** tab, define your network device, then click **Add**.  
You return to the **Network Devices** dialog, where the new device is listed.
3. Click **Export All**.  
The **Export to File** dialog opens.

**Figure 14** Export to File Dialog



4. **Export file with password protection:** Select **No**.
5. Click **Export**.

6. Download the XMLfile to your system.
7. Open the XML file in a text editor to view the format.

## Adding a ClearPass/RADIUS Server to the Mobility Controller

The ClearPass Policy Manager server is a RADIUS server. You must add a ClearPass/RADIUS server to the mobility controller because doing so allows ClearPass to be integrated with the mobility controller and the wireless LAN authentication process.

By adding the ClearPass/RADIUS server to the mobility controller, you are configuring the mobility controller to send authentication requests to the ClearPass/RADIUS server.

To define the ClearPass/RADIUS server in the mobility controller so that it can be used for any RADIUS authentication task:

1. Log in to the Mobility Controller.
2. Select the **Configuration** tab.
3. In the left navigation pane, select **SECURITY > Authentication**.  
The **Security > Authentication > Servers** screen opens.
4. Choose **RADIUS Server**.  
The action list of existing RADIUS servers is displayed.
5. To add a RADIUS server, enter the name of the new RADIUS server in the **Add** text box (at the bottom of the screen), then click **Add**.

**Figure 15 Defining the RADIUS Server in the Mobility Controller**

The screenshot shows the 'Security > Authentication > Servers' interface. On the left, there's a navigation pane with tabs: Servers, AAA Profiles, L2 Authentication, L3 Authentication, User Rules, and Advanced. Under 'Servers', the 'RADIUS Server' tab is selected, showing a list of existing servers: gchit-radius-server-guest, isam-aso-idp-cppm, isam-aso-idp-radius, ouma-airgroup-server, ouma-radius-server, ouma2-radius-server, qa-onboard, rajeev-airgroup-radius, rajeev-onboard-radius, rajeev-radius-server, rajeev-social-server, rashmi-social-server, sdas-cpg-qa-radius, sdas-dot1x-radius, sham-cpg-qa-radius, sham-onboard-radius, and sham-onguard-radius. At the bottom of the list, there's an 'Add' text box containing 'ClearPass\_3' and an 'Add' button. The entire interface has a light blue background with white text and blue buttons.

The new server is added to the **RADIUS Server** list.

6. Click the name of the new RADIUS server.  
The **RADIUS Server** configuration screen opens.

**Figure 16** Configuring the RADIUS Server

7. Specify the values for the RADIUS server configuration parameters as described in [Table 7](#).

**Table 7:** Configuring RADIUS Server Parameters on the Mobility Controller

RADIUS Server Parameter	Action/Description	Comments
Host	<p>Specify the IP address or the fully qualified domain name of the RADIUS server.</p> <p><b>NOTE:</b> In this case, specify the IP address of the ClearPass server, which is a RADIUS server.</p>	When you first add the RADIUS server, the mobility controller populates the <b>Host</b> field with a dummy IP address—127.0.0.1.
Key	<p>Enter the RADIUS shared secret that is configured on the authentication server (in this case, the ClearPass server).</p> <p><b>NOTE:</b> The RADIUS <b>Key</b> value on the controller and the <b>RADIUS Shared Secret</b> on the ClearPass server must be identical.</p>	The maximum length is 128 characters.
CPPM credentials	Enter the ClearPass server credentials if you want the mobility controller to use a configurable username and password instead of a support password.	
Auth Port	Specify the authentication port on the RADIUS server.	<ul style="list-style-type: none"> <li>Range: 1 to 65535</li> <li>Default: 1812</li> </ul>
Acct Port	Specify the accounting port on the RADIUS server.	<ul style="list-style-type: none"> <li>Range: 1 to 65535</li> <li>Default: 1813</li> </ul>

RADIUS Server Parameter	Action/Description	Comments
Radsec Port	Specify the Radsec (Secure RADIUS Service) port number of this server.	<ul style="list-style-type: none"> <li>Range: 1 to 65535</li> <li>Default: 2083</li> </ul>
Retransmits <number>	Enter the maximum number of retries sent to the server by the mobility controller before the server is marked as down.	<ul style="list-style-type: none"> <li>Range: 0 to 3</li> <li>Default: 3</li> </ul>
Timeout <seconds>	Enter the maximum time, in seconds, that the mobility controller waits before timing out the request and resending it.	<ul style="list-style-type: none"> <li>Range: 0 to 30</li> <li>Default: 5</li> </ul>
NAS ID	Optional: Enter the Network Access Server (NAS) identifier to use in RADIUS packets. The NAS in this case is the Mobility Controller.	The NAS ID should be unique to the controller within the scope of the RADIUS server. For example, a fully qualified domain name is suitable as a NAS ID.
NAS IP	<p>Specify the NAS IP address to send in RADIUS packets.</p> <ul style="list-style-type: none"> <li>To set the global NAS IP address, enter the following command: <code>ip radius nas-ip &lt;ip_addr&gt;</code></li> </ul>	You can configure a global NAS IP address that the mobility controller uses for communications with all RADIUS servers. If you do not configure a server-specific NAS IP address, the global NAS IP address is used.
Enable IPv6	To enable the operation of the RADIUS server over IPv6, check the <b>Enable IPv6</b> check box.	Enabling IPv6 also enables the RADIUS attributes used to support IPv6 network access.
Source Interface	<p>Enter a VLAN number ID.</p> <p>This allows you to use source IP addresses to differentiate RADIUS requests.</p> <ul style="list-style-type: none"> <li><b>VLAN ID:</b> Specify <b>vlanid</b> for the source interface when the RADIUS packets are sent to the RADIUS server via IPv4.</li> <li><b>IPv6 address:</b> Specify <b>ipv6addr</b> for the source interface when the RADIUS packets are sent to the RADIUS/ClearPass Policy Manager server via IPv6.</li> </ul> <p><b>NOTE:</b> A VLAN interface can have multiple IPv6 addresses, which is why it isn't sufficient to specify the VLAN ID for RADIUS over IPv6.</p>	<p>This option associates a VLAN interface with the RADIUS server to allow the server-specific source interface to override the global configuration. This option defines the source IP address in the RADIUS requests.</p> <ul style="list-style-type: none"> <li>If you associate a Source Interface (by entering a VLAN number) with a configured server, then the source IP address of the packet is that interface's IP address.</li> <li>If you do not associate the Source Interface with a configured server (by leaving the field blank), the IP address of the global Source Interface</li> </ul>

RADIUS Server Parameter	Action/Description	Comments
		is used.
Use MD5	Enable this option to use an MD5 hash instead of a clear text password.	This option is disabled by default.
Use IP address for calling station ID	Enable this option if you choose to use an IP address instead of a MAC address for calling station IDs.	This option is disabled by default.
Mode	Enable this option if you want to enable the RADIUS server.	The <b>Mode</b> parameter defines whether the controller should or should not send RADIUS requests to the RADIUS/ClearPass server. This option is enabled by default.
Lowercase MAC address	Sends the MAC address in lowercase in the authentication and accounting requests to this server.	Default: Disabled
MAC address delimiter	Optionally, specify a MAC address delimiter.  Sends the MAC address with the following delimiters in the authentication and accounting requests of this server: <ul style="list-style-type: none"><li>● <b>colon</b>: Send MAC address as: XX:XX:XX:XX:XX:XX</li><li>● <b>dash</b>: Send MAC address as: XX-XX-XX-XX-XX-XX</li><li>● <b>none</b>: Send MAC address as: XXXXXXXXXXXX</li><li>● <b>oui-nic</b>: Send MAC address as: XXXXX-XXXXXX</li></ul>	Default: None
Service-type of FRAMED-USER	Enable this option to send the service-type as <b>FRAMED-USER</b> instead of <b>LOGIN-USER</b> .	Default: Disabled
Radsec	Enable or disable RADIUS over TLS (Secure RADIUS Service) for this server.	Default: Disabled
Radsec Trusted CA Name	Enter the trusted Certificate Authority (CA) name to be used to verify this server.	
Radsec Server Cert Name	Enter the name of the trusted Radsec server certificate.	
Radsec Client Cert	Enter the name of the Radsec client certificate that the mobility controller should use for Radsec requests.	

RADIUS Server Parameter	Action/Description	Comments
called-station-id	<p>Specify the MAC address of the mobility controller. This parameter allows you to send different values for <b>Called Station ID</b>.</p> <p>Configure the following parameters:</p> <ul style="list-style-type: none"> <li>● <b>csid_type</b>: Called station ID type. Default: macaddr</li> <li>● <b>include_ssid</b>: Enabling this option includes the SSID in the <b>Called Station ID</b> along with <b>csid_type</b>. Default: Disabled</li> <li>● <b>csid_delimiter</b>: Enabling this option allows you to send this delimiter to separate <b>csid_type</b> and <b>ssid</b> in the <b>Called Station ID</b>. Default: colon (Example: 00-1a-1e-00-1a-b8:dotx-ssid)</li> </ul>	

- When finished, click **Apply**.

The following message is displayed:

*Configuration Updated successfully*

## Adding the ClearPass/RADIUS Server to a Server Group

Before you can reference the ClearPass/RADIUS server in the configuration, you must add the ClearPass/RADIUS server to a server group.

- You can add multiple RADIUS servers in a server group. You can configure the same server in more than one server group. Note that you must configure a server before you can include it in a server group. Server names must be unique.




---

Even if there is only one RADIUS server, you must add it to a RADIUS server group.

---

- You can create groups of RADIUS servers for specific types of authentication—for example, you can specify one or more RADIUS servers to be used for 802.1x authentication.
- You can also configure servers of different types in one server group. For example, you can include the internal database as a backup to a RADIUS server.

To add the ClearPass/RADIUS server to a server group:

1. On the mobility controller, select the **Configuration** tab.
2. In the navigation pane, select **SECURITY > Authentication**.  
The **Authentication > Servers** screen opens.
3. From the list of server types on the left side of the screen, select **Server Group**.  
The **Server Group** page opens.

**Figure 17** Server Group Page

The screenshot shows the 'Configuration' tab selected in the top navigation bar. Below it, the 'Security > Authentication > Servers' path is visible. A sub-navigation bar includes 'Servers', 'AAA Profiles', 'L2 Authentication', 'L3 Authentication', 'User Rules', and 'Advanced'. On the left, a sidebar lists 'Server Group' (with 'default' and 'internal' entries), 'RADIUS Server', and 'LDAP Server'. The main panel displays a table titled 'Server Group' with columns 'Instance', 'Servers out of Service', and 'Actions'. It contains two rows: 'default' and 'internal', each with 'Show Reference' and 'Delete' buttons. Below the table is a text input field containing 'ClearPassGroup1' and an 'Add' button.

4. To add a server group, enter the name of the server group in the **Add** field, then click **Add**.  
The new server group you defined is now included in the **Server Group** list.
5. To configure the server group, click the **name of the new server group**.  
The configuration screen for the selected server group opens.

**Figure 18** Server Group Configuration Screen

The screenshot shows the 'Server Group > ClearPassGroup1' configuration screen. At the top right are 'Show Reference', 'Save As', and 'Reset' buttons. The screen is divided into sections: 'Fail Through' and 'Load Balance' (both with checkboxes); 'Servers' (with 'Name', 'Server-Type', 'trim-FQDN', and 'Match-Rule' columns and 'New', 'Delete' buttons); and 'Server Rules' (with 'Priority', 'Attribute', 'Operation', 'Operand', 'Type', 'Action', 'Value', and 'Validated' columns and 'New', 'Delete' buttons).

6. To add a ClearPass Policy Manager server to the server group, in the **Servers** section, click **New**.  
The **Servers** configuration screen opens.
7. To choose the ClearPass server for inclusion in the RADIUS server group, select the ClearPass (RADIUS) server name from the drop-down list (see [Figure 19](#)).

**Figure 19** Selecting the ClearPass Server for Inclusion in the RADIUS Server Group

Name	Server Name	Server-Type	trim-FQDN	Match Rules
Internal (Local)				
Internal (Local)				
ClearPass1 (Radius)		Radius	No	

The new RADIUS server name is now displayed in the **Server Name** list.

8. If necessary, modify the **Servers** settings as needed, then click **Add Server**.

You return to the **Server Group** configuration screen. The ClearPass Policy Manager server is now included in the RADIUS server group.

**Figure 20** ClearPass Server Added to the RADIUS Server Group

Name	Server Name	Server-Type	trim-FQDN	Match Rules
ClearPass1		Radius	No	

9. Click **Apply**, then from the top of the screen, click **Save Configuration**.

You have now defined the ClearPass server as a RADIUS server, and the RADIUS server is a member of a RADIUS server group. These tasks are required before you can use the ClearPass Policy Manager server as a RADIUS server in the network.

## Using the CLI

To use the CLI to add a server to a server group:

```
(Controller-1) (config) #aaa server-group <name> auth-server <name>
```

## Configuring an AAA Profile for 802.1X Authentication

The AAA profile configures the authentication for a Wireless LAN. The AAA profile defines the type of authentication (in this example, 802.1x), the authentication server group, and the default user role for

authenticated users.



Be sure to assign a unique name to each virtual AP, SSID, and AAA profile that you modify.

With the RADIUS server and RADIUS server group configured, you can now configure an AAA profile that will refer to that server group, which, in turn, refers to a server in that server group.

To configure an AAA profile:

1. On the mobility controller, navigate to **Configuration > SECURITY > Authentication > AAA Profiles** tab.  
The AAA Profiles Summary is displayed.

**Figure 21** AAA Profiles Summary

AAA Profiles Summary							
Name	Role	MAC Auth.	802.1x Auth.	RADIUS Acct.	XML-API Auth.	RFC 3576 Auth.	Actions
david	logon						<a href="#">Show Reference</a> <a href="#">Delete</a>
davidtest-aaa_prof	authenticated						<a href="#">Show Reference</a> <a href="#">Delete</a>
default	logon					10.0.0.1	<a href="#">Show Reference</a> <a href="#">Delete</a> <a href="#">Show Reference</a>

2. To add a new AAA profile, scroll to the bottom of the screen and click **Add**.
3. Enter the name of the AAA profile in the **Add** text box, then click **Add**.
4. Scroll to the name of the new AAA profile and click the profile name.  
The **AAA Profiles** configuration page opens, with the list of existing AAA profiles displayed on the left.
5. Expand the menu to view the desired AAA profile, then select the profile.  
The **AAA Profile Configuration** page opens.

**Figure 22** AAA Profile Configuration Page

The screenshot shows the 'AAA Profile Configuration Page' with the 'AAA Profiles' tab selected. On the left, a tree view shows the hierarchy under 'AAA', including 'ClearPassAAAProfile' which is expanded to show 'MAC Authentication', 'MAC Authentication Server Group default', '802.1X Authentication', '802.1X Authentication Server Group', 'RADIUS Accounting', 'XML API server', 'RFC 3576 server', and several user profiles ('david', 'davidtest-aaa\_prof', 'default', 'default-dot1x', 'default-dot1x-psk', 'default-mac-auth'). The main panel displays the configuration for 'ClearPassAAAProfile'. It includes fields for 'Initial role' (set to 'logon'), 'MAC Authentication Default Role' (set to 'guest'), '802.1X Authentication Default Role' (set to 'guest'), and various other settings like 'User idle timeout' (disabled), 'Max IPv4 for wireless user' (set to 2), and 'Wired to Wireless Roaming' (checked). Buttons for 'Show Reference', 'Save As', and 'Reset' are at the top right.

- Configure the AAA profile parameters according to your particular use case (refer to [Table 8](#) below for AAA profile parameter details).

**Table 8:** Configuring AAA Profile Parameters

AAA Profile Parameter	Action/Description	Comments
Initial role	1. Click the <b>Initial Role</b> drop-down list and select a role for unauthenticated users.	The default role for unauthenticated users is <b>logon</b> .
MAC Authentication Default Role	2. Click the <b>MAC Authentication Default Role</b> drop-down list and select the role assigned to the user when the device is MAC authenticated.	<p>The default role for MAC authentication is the <b>guest</b> user role. If derivation rules are present, the role assigned to the client through these rules takes precedence over the default role.</p> <p><b>NOTE:</b> This feature requires a Policy Enforcement Firewall Next Generation (PEFNG) license.</p>

AAA Profile Parameter	Action/Description	Comments
Download Role from CPPM	<p>3. Enable the <b>Download Role from CPPM</b> option.</p> <p>When you enable this option, the configured ClearPass/RADIUS server provides the role name at user authentication.</p>	The authenticator controller can request the role details if the role does not exist. Users are then assigned to the newly-defined role.
Layer-2 Authentication Fail Through	<p>4. Enable this option to enable the <b>L2-authentication-failthrough</b> mode.</p> <ul style="list-style-type: none"> <li>When this option is enabled, the 802.1X authentication is allowed even if MAC authentication fails.</li> <li>If this option is disabled, 802.1X authentication is not allowed.</li> </ul>	<b>L2-authentication-failthrough</b> mode is disabled by default.
User idle timeout	<p>5. Select the <b>Enable</b> check box to configure the <b>user idle timeout</b> value for this AAA profile.</p> <p>a. Specify the idle timeout value for the client in the number of seconds.</p>	<p>Enabling this option overrides the global settings configured in the AAA timers.</p> <ul style="list-style-type: none"> <li>If this is disabled, the global settings are applied.</li> <li>Range: 30 to 15300 in multiples of 30 seconds.</li> <li>A value of <b>0</b> deletes the user immediately after disassociation from the wireless network.</li> </ul>
Max IPv4 for wireless user	<p>6. Specify the number of IPv4 addresses that can be associated to a wireless user.</p> <p>Inter-controller mobility does not support more than two IP addresses per wireless user.</p> <p>Upon configuration, the following warning is issued:</p> <p><i>Warning: Increased max-IP limit can keep system from scaling to max users on all master and local controllers.</i></p>	<ul style="list-style-type: none"> <li>Minimum: 1</li> <li>Maximum: 32</li> <li>Default: 2</li> </ul>
RADIUS Interim Accounting	7. Enable this option to allow the mobility controller to send Interim-Update messages with current user statistics to the RADIUS accounting server at regular intervals.	This option is disabled by default, allowing the mobility controller to send only start and stop messages to the RADIUS accounting server.
User derivation rules	8. Click the <b>User derivation rules</b> drop-down list to specify a user attribute profile from which the user role or VLAN is derived.	

AAA Profile Parameter	Action/Description	Comments
Wired to Wireless Roaming	9. Enable this feature to keep users authenticated when they roam from the wired side of the network.	This feature is enabled by default.
SIP authentication role	10. To specify the role assigned to a Session Initiation Protocol (SIP) client upon registration, click the <b>SIP authentication role</b> drop-down list.	<b>NOTE:</b> This feature requires a Policy Enforcement Firewall Next Generation (PEFNG) license.
Device Type Classification	11. Enable this option to configure the mobility controller to parse user-agent strings and identify the type of device connecting to the access point.	When the device type classification is enabled, the <b>Global Clients</b> table shown in the <b>Monitoring &gt; Network &gt; All WLAN Clients</b> window shows each client's device type (if the client device can be identified).
Enforce DHCP	12. Enable this option when you create a user rule that assigns a specific role or VLAN based upon the client device's type. <b>NOTE:</b> If a client is removed from the user table by the "Logon user lifetime" AAA timer, that client will not be able to send traffic until it renews the DHCP lease.	When you select this option, clients must obtain an IP address using the Dynamic Host Configuration Protocol (DHCP) before they are allowed to associate to an access point.
PAN Firewalls Integration	13. Enable this option to require mapping the IP addresses of Palo Alto Networks firewalls.	
Open SSID RADIUS Accounting	14. Enable this option to have a Network Access Server (NAS) operate as a client of the RADIUS accounting server. The client is responsible for passing user accounting information to a designated RADIUS accounting server.	The RADIUS accounting server can act as a proxy client to other kinds of accounting servers. Transactions between the client and the RADIUS accounting server are authenticated through the use of a shared secret, which is never sent over the network.
	15. When you are finished with the AAA profile settings, click <b>Apply</b> .	

This completes the AAA profile configuration for 802.1X authentication.

# Configuring a Virtual AP Profile

This section contains the following information:

- [About Virtual AP Profiles](#)
- [Configuring the Virtual AP Profile](#)

## About Virtual AP Profiles

Access points (APs) advertise Wireless LANs to wireless clients by sending out beacons and probing responses that contain the Wireless LAN's SSID and the supported authentication and data rates. When a wireless client associates to an AP, it sends traffic to the AP's Basic Service Set Identifier (BSSID), which is usually the AP's MAC address.

In an Aruba network, an access point uses a unique BSSID for each Wireless LAN. Thus, a physical AP can support multiple WLANs. The WLAN configuration applied to a BSSID on an AP is called a *virtual AP*.

You can configure and apply multiple virtual APs to an AP group or to an individual AP by defining one or more *virtual AP profiles*. You can configure virtual AP profiles to provide different network access or services to users on the same physical network.

- For example, you can configure a Wireless LAN to provide access to guest users and another WLAN to provide access to employee users through the same APs.
- You can also configure a Wireless LAN that offers open authentication and Captive Portal access with data rates of 1 MBps and 2 MBps, and another Wireless LAN that requires Wi-Fi Protected Access (WPA) authentication with data rates of up to 11 MBps.

## Example

As an example, suppose there are users in both Edmonton and Toronto that access the same "Corpnet" Wireless LAN.

If the Wireless LAN required authentication to an external server, users who associate with the APs in Toronto would want to authenticate with their local servers.

In this case, you can configure two virtual APs that each reference a slightly different AAA profile—one AAA profile that references authentication servers in Edmonton and the other AAA profile that references servers in Toronto (see [Table 9](#)).

When you create a Wireless LAN using the mobility controller's WLAN wizard, the mobility controller automatically creates a Virtual AP profile (VAP) based on the Wireless LAN's configuration.



The name the mobility controller assigns to the VAP is the name of the WLAN with "-vap\_prof" appended to the name. For example, the VAP for a Wireless LAN named "802.1X-CP" would be named "802.1X-CP-vap\_prof."

**Table 9: Applying WLAN Profiles to AP Groups**

WLAN Profiles	Default AP Group	Toronto AP Group
Virtual AP	Corpnet-Ed	Corpnet-Tr
SSID	Corpnet	Corpnet
AAA	Ed-Servers	Tr-Servers

You can apply multiple virtual AP profiles to individual APs. You can also apply the same virtual AP profile to one or more AP groups.

## Configuring the Virtual AP Profile

To configure the Virtual AP profile:

1. On the mobility controller, navigate to **Configuration > ADVANCED SERVICES > All Profiles**.
2. Expand the *Wireless LAN* profile and select **Virtual AP**.  
The list of existing Virtual AP profiles appears in the **Profile Details** pane.
3. Scroll to the Virtual AP profile based on the Wireless LAN you created, then select it.
  - To configure an existing Virtual AP profile, select the name of the profile in the **Profile Details** pane.
  - To create a new Virtual AP profile:
    - a) Enter a name for the profile in the entry field at the bottom of the **Profile Details** pane, then click **Add**.
    - b) Select the name of the profile in the **Profile Details** pane.



Whenever you create a new virtual AP profile in the WebUI, the profile automatically contains the “default” SSID profile with the default “Aruba-ap” ESSID. You must configure a new ESSID and SSID profile for the virtual AP profile before you apply the profile (for related information , see [Adding an SSID to the Mobility Controller for 802.1X Authentication on page 54](#)).

The **Virtual AP Profile** configuration screen opens.

**Figure 23** Virtual AP Profile Configuration Screen

The screenshot shows the 'Advanced Services > All Profile Management' screen. At the top, there are tabs for Configuration, Diagnostics, Maintenance, and Save Configuration. The Configuration tab is selected. Below the tabs is a breadcrumb trail: 'Virtual AP profile > dot1x-cp-vap\_prof'. To the right of the breadcrumb are three buttons: Show Reference, Save As, and Reset. The main area is divided into two panes: 'Profiles' on the left and 'Profile Details' on the right. The 'Profiles' pane lists several profiles, including 'dot1x-cp-vap\_prof' which is expanded to show its sub-profiles: AAA, 802.11K, Hotspot 2.0, SSID, and WMM Traffic Management. The 'Profile Details' pane displays the configuration for the selected profile. It has tabs for Basic and Advanced, with Basic selected. Under the General tab, 'Virtual AP enable' is checked, 'VLAN' is set to 1, and 'Forward mode' is set to tunnel. Under the RF tab, 'Allowed band' is set to a, 'Band Steering' is off, and 'Steering Mode' is prefer-Sghz. Under the Broadcast/Multicast tab, 'Dynamic Multicast Optimization (DMO)' is off, 'Drop Broadcast and Multicast' is off, and 'Convert Broadcast ARP requests to unicast' is checked. There are also tabs for 'AAA', '802.11K', 'SSID', and 'WMM Traffic Management' on the right side of the profile details pane.

The list of profiles on the left of [Figure 23](#) shows all the settings associated with the selected virtual AP profile—**AAA profile** (which contains the RADIUS information), **802.11K**, and **SSID** settings.

4. Configure the profile parameters described in [Table 10](#).

The virtual AP profile is divided into two tabs:

- **Basic:** Displays only those configuration settings that often need to be adjusted to suit a specific network.
- **Advanced:** Shows all configuration settings, including settings that do not need frequent adjustment or should be kept at their default values.

For details on the advanced virtual AP profile parameters, refer to the *ArubaOS User Guide > Virtual APs* chapter > *Table: "Virtual AP Profile Parameters."*



If you change a setting on one tab, then click and display the other tab without saving your changed configuration, that changed setting reverts to its previous value.

**Table 10: Basic Virtual AP Profile Parameters**

VAP Parameter	Action/Description
<b>General</b>	
Virtual AP enable	<ol style="list-style-type: none"> <li>Select the <b>Virtual AP enable</b> check box to enable or disable the virtual AP. This feature is enabled by default.</li> </ol>
VLAN	<ol style="list-style-type: none"> <li>Specify the VLAN(s) into which users are placed in order to obtain an IP address. To associate that VLAN with the virtual AP profile:             <ol style="list-style-type: none"> <li>Click the drop-down list to select a configured VLAN.</li> <li>Click the <b>Arrow</b> button.</li> </ol> </li> </ol>
Forward mode	<p>The Forward mode parameter controls whether data is tunneled to the mobility controller using generic routing encapsulation (GRE), bridged into the local Ethernet LAN (for remote APs), or a combination thereof depending on the destination—corporate traffic goes to the mobility controller, and Internet access remains local.</p> <p>All forwarding modes support band steering, Traffic Specification (TSPEC) and Traffic Classification (TCLAS) enforcement, 802.11k, and station blacklisting.</p> <ol style="list-style-type: none"> <li>Click the drop-down list to select one of the following forward modes:             <ul style="list-style-type: none"> <li><b>Tunnel:</b> The AP handles all 802.11 association requests and responses, but it sends all 802.11 data packets, action frames, and Extensible Authentication Protocol Over LAN (EAPOL) frames over a GRE tunnel to the mobility controller for processing. You can configure both remote and campus APs in tunnel mode.</li> <li><b>Bridge:</b> 802.11 frames are bridged into the local Ethernet LAN. Both remote and campus APs can be configured in Bridge mode. You must enable the control plane security feature on the mobility controller before you configure campus APs in bridge mode.</li> <li><b>Split-Tunnel:</b> 802.11 frames are either tunneled or bridged, depending on the destination.</li> </ul> </li> </ol> <p><b>NOTE: Decrypt-Tunnel:</b> Both remote and campus APs can be configured in decrypt-tunnel mode. When an AP uses decrypt-tunnel forwarding mode, that AP decrypts and decapsulates all 802.11 frames from a client and sends the 802.3 frames through the GRE tunnel to the mobility controller, which then applies firewall policies to the user traffic.</p> <p><b>NOTE:</b> Before you configure campus APs in decrypt-tunnel forward mode, you must enable the <b>Control Plane Security</b> feature on the mobility controller.</p>
<b>RF</b>	
Allowed band	<ol style="list-style-type: none"> <li>Specify the band on which to use the virtual AP:             <ul style="list-style-type: none"> <li><b>a</b>—802.11a band only (5 GHz)</li> </ul> </li> </ol>

VAP Parameter	Action/Description
	<ul style="list-style-type: none"> <li><b>g</b>—802.11b/g band only (2.4 GHz)</li> <li><b>all</b>—Both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz) The default band setting is <b>all</b>.</li> </ul>
Band Steering	<p>5. Enable the Band Steering parameter to reduce co-channel interference and increase available bandwidth for dual-band clients (because there are more channels on the 5GHz band than on the 2.4GHz band).</p> <ul style="list-style-type: none"> <li>This feature supports both campus APs and remote APs that have a virtual AP profile set to tunnel, split-tunnel, or bridge forwarding mode.</li> <li>This feature is disabled by default, and must be enabled in a virtual AP profile.</li> </ul>
Steering Mode	<p>6. Specify the Band Steering mode:</p> <ul style="list-style-type: none"> <li><b>Force-5GHz</b>: When the AP is configured in force-5GHz band steering mode, the AP tries to force 5Ghz-capable APs to use that radio band.</li> <li><b>Prefer-5GHz</b> (Default): If you configure the AP to use <b>Prefer-5GHz</b> band steering mode, the AP tries to steer the client to the 5G band (if the client is 5G capable), but the AP lets the client connect on the 2.4G band if the client persists in 2.4G association attempts.</li> <li><b>Balance-bands</b>: The AP balances the clients across the two radios to best utilize the available 2.4G bandwidth.</li> </ul>
<b>Broadcast/Multicast</b>	
Dynamic Multicast Optimization (DMO)	<p>7. Select this check box to enable <b>Dynamic Multicast Optimization</b>. This parameter is disabled by default, and cannot be enabled without the Policy Enforcement Firewall Next Generation (PEFNG) license.</p>
Drop Broadcast and Multicast	<p>8. Select the <b>Drop Broadcast and Multicast</b> check box to filter out broadcast and multicast traffic in the air.</p> <p><b>NOTE:</b> Do not enable this option for virtual APs configured in bridge-forwarding mode. This configuration parameter is to be used only for virtual APs in tunnel mode. In tunnel mode, all packets travel to the controller, so the controller is able to drop all broadcast traffic. When a virtual AP is configured to use bridge-forwarding mode, most data traffic stays local to the AP, and the controller is not able to filter out that broadcast traffic.</p> <p><b>IMPORTANT:</b> If you enable this option, you must also enable the <b>Broadcast-Filter ARP</b> parameter on the virtual AP profile to prevent ARP requests from being dropped. You can enable this parameter by checking the <b>Convert Broadcast ARP requests to unicast</b> check box as described in the following parameter (<b>Convert Broadcast ARP requests to unicast</b>).</p>
Convert Broadcast ARP requests to unicast	<p>9. Enable this option to convert all broadcast ARP requests to unicast and sent directly to the client. You can check the status of this option using the <b>show ap active</b> and the <b>show datapath tunnel</b> commands. The output displays the letter <b>a</b> in the Flags column. The <b>Convert Broadcast ARP requests to unicast</b> option includes the additional functionality of a <b>broadcast-filter all</b> parameter, where DHCP response frames are sent as unicast to the corresponding client.</p> <p><b>NOTE:</b> This option, when enabled, can impact DHCP discover packets, requested</p>

VAP Parameter	Action/Description
	<p>packets for clients that are behind a wireless bridge, and virtual clients on VMware devices.</p> <ul style="list-style-type: none"> <li>To resolve this issue and allow clients that are behind a wireless bridge or VMware devices to receive an IP address, disable this option. This parameter is enabled by default.</li> </ul>
	10. When finished specifying the Virtual AP profile settings, click <b>Apply</b>

This completes the configuration for the Virtual AP Profile.

## Configuring ClearPass as an RFC 3576 (CoA) Server

This section contains the following information:

- [About the CoA Server](#)
- [Configuring the ClearPass Server as a CoA Server](#)
- [Using the CLI](#)

### About the CoA Server

This section describes how to configure the ClearPass server as a CoA (Change of Authorization) server.

You can configure a RADIUS server to send user disconnect, change of authorization (CoA), and session-timeout messages as described in RFC 3576, “Dynamic Authorization Extensions to Remote Dial In User Service (RADIUS).”

The disconnect, session timeout, and change of authorization messages sent from the server to the mobility controller contain information to identify the user for whom the message is sent.

The mobility controller supports the following attributes for identifying the users who authenticate with an RFC 3576 server:

- **user-name:** Name of the user to be authenticated.
- **framed-ip-address:** User’s IP address.
- **calling-station-id:** Phone number of a station that originated a call.
- **accounting-session-id:** Unique accounting ID for the user session.

If the authentication server sends both supported and unsupported attributes to the mobility controller, the unknown or unsupported attributes are ignored.

If no matching user is found, the mobility controller sends a *503: Session Not Found* error message back to the RFC 3576 server.

### Configuring the ClearPass Server as a CoA Server

To configure the ClearPass server as a CoA server:

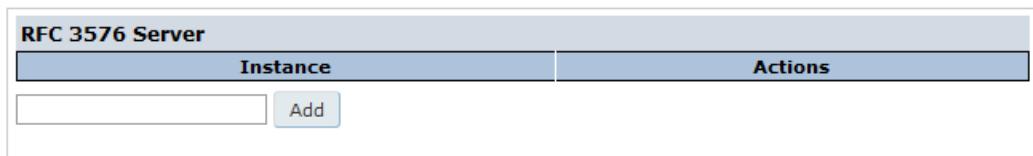


Before you configure any server as a CoA server, RADIUS CoA must be enabled on the device (for details, see [Adding a Mobility Controller to ClearPass Policy Manager](#)).

1. On the mobility controller, navigate to **Configuration > SECURITY > Authentication**.  
The **Servers** tab is displayed by default.

2. To display the list of RFC 3576 servers, select **RFC 3576 Server**.
3. If the ClearPass server's IP address is not already listed in the list of RFC 3576 servers, enter the IP address of the ClearPass server in the **Add** text box, then click **Add**.

**Figure 24** Adding an RFC 3576 Server



The IP address of the ClearPass server is displayed in the list of RFC 3576 servers.

4. To configure the server parameters, click the name (which is the IP address) of the newly created RFC 3576 server.

The following dialog appears.

**Figure 25** Setting 3576 Server Parameters

Show Reference   Save As   Reset

Key	
Key:	*****
Retype:	*****
Radsec	
<input checked="" type="checkbox"/>	

5. Specify the parameters for the RFC 3576 server.

- a. **Key** parameter: Enter and verify the RADIUS shared key.

This key value is the same RADIUS key value configured for the mobility controller.

 To enable communication between the mobility controller and the ClearPass server, the values for RADIUS key configured on the mobility controller and the RADIUS shared secret configured on the ClearPass server must be identical.

- b. **Radsec** check box: Enable or disable RADIUS over TLS for this server.

6. When finished, click **Apply**.

The following message is displayed: *Configuration Updated successfully*.

The new RFC 3576 server is listed on the Servers list.

## Using the CLI

Use the following commands to configure an RFC 3576 server using the CLI:

```
aaa rfc-3576-server <server_IP_address>
key <string>
```

For example:

```
(controller) (config) #aaa rfc-3576-server 10.100.8.32
(controller) (RFC 3576 Server "10.100.8.32") #key employee123
```

# Adding an SSID to the Mobility Controller for 802.1X Authentication

This section describes how to create and configure a Service Set Identifier (SSID) to the mobility controller for 802.1X authentication.

This section contains the following information:

- [SSID Profile Overview](#)
- [Adding an SSID to the Mobility Controller](#)

## SSID Profile Overview

An SSID (Service Set Identifier) is the name of the network or Wireless LAN that clients see. An SSID profile defines the name of the network, authentication type for the network, basic rates, transmit rates, SSID cloaking, and certain wireless multimedia settings for the network.

ArubaOS supports different types of the Advanced Encryption Standard (AES), Temporal Key Integrity Protocol (TKIP), and wired equivalent privacy (WEP) encryption. AES is the most secure and the recommended encryption method.

Most modern devices are AES-capable, and therefore AES should be the default encryption method. Use TKIP only when the network includes devices that do not support AES. In these situations, use a separate SSID for devices that are only capable of TKIP.

## Adding an SSID to the Mobility Controller

This section assumes that the mobility controller's basic configuration has been completed as described in the previous sections of this chapter, and that the access points (APs) have been provisioned.

To add an SSID for 802.1X authentication:

1. On the mobility controller, navigate to **Configuration > WIZARDS > Campus WLAN**.  
The **Configure WLAN** wizard opens.

**Figure 26** Specifying the Wireless LAN



2. From the **AP Groups** pane, select the appropriate AP group, or click **New** to create a new AP group.
3. From the **WLANS for <name>** pane, select the Wireless LAN you wish to use, or click **New** to create a new Wireless LAN.
4. In the **Create New WLAN Named** dialog, enter the name of the new Wireless LAN.

**Figure 27** Creating a New Wireless LAN



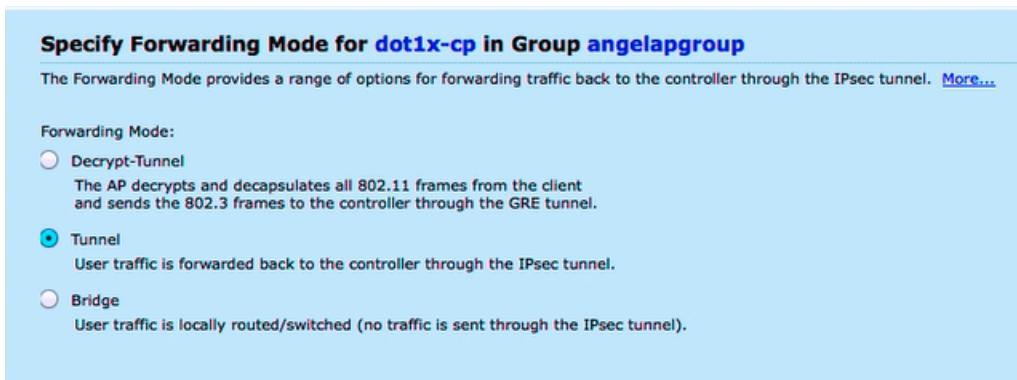
- To proceed, press **OK**.

The new Wireless LAN is added to the list of Wireless LANs. Note that the **New**, **Copy**, **Delete**, and **Share** buttons are now enabled.

- To begin configuration for the new Wireless LAN, press **Next**.

The **Specify Forwarding Mode** configuration screen opens.

**Figure 28** Specifying Forwarding Mode

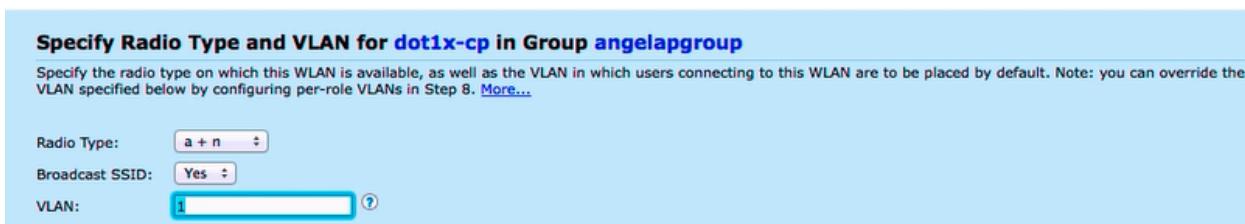


- The forwarding mode selected for a mobility controller affects how much traffic and how many tunnels the AP will generate.
- The default mode is *Tunnel forwarding mode*, in which traffic is forwarded to the mobility controller through an IPsec tunnel.

- Select the forwarding mode, then click **Next**.

The **Radio Type and VLAN** configuration screen opens.

**Figure 29** Specifying Radio Type and VLAN ID



8. Enter the values to specify the radio type and VLAN, then click **Next**.
  - a. **Radio Type:** This allows you to specify which radio frequencies the SSID will broadcast on. The **a+n** radio type is selected in this example because this radio type specifies the 5 GHz spectrum, which has more bandwidth than the 2.4 GHz spectrum.
  - b. **Broadcast SSID:** Indicate by **Yes** or **No** whether you want to broadcast this SSID.
  - c. **VLAN:** Choose the VLAN that the user will be assigned to after a successful authentication. VLAN IDs are suggested from the drop-down list of currently configured VLANs. You can select multiple VLANs by separating them with commas.

The **Specify Usage Scenario** configuration screen opens.

**Figure 30** Specifying the WLAN Usage Scenario



This screen specifies whether this Wireless LAN is for guest usage (and therefore, captive portal authentication), or for Internal usage (802.1X authentication).

9. Specify **Internal** (the default setting), then click **Next**.

The **Specify Authentication and Encryption** configuration screen opens.

**Figure 31** Setting Up Authentication and Encryption



10. For this step, do the following:

- a. Specify **Strong encryption with 802.1X authentication**.
- b. Accept the default settings for **Authentication: WPA-2Enterprise** and **Encryption: aes**, then click **Next**.

The **Specify Authentication Server** screen opens.

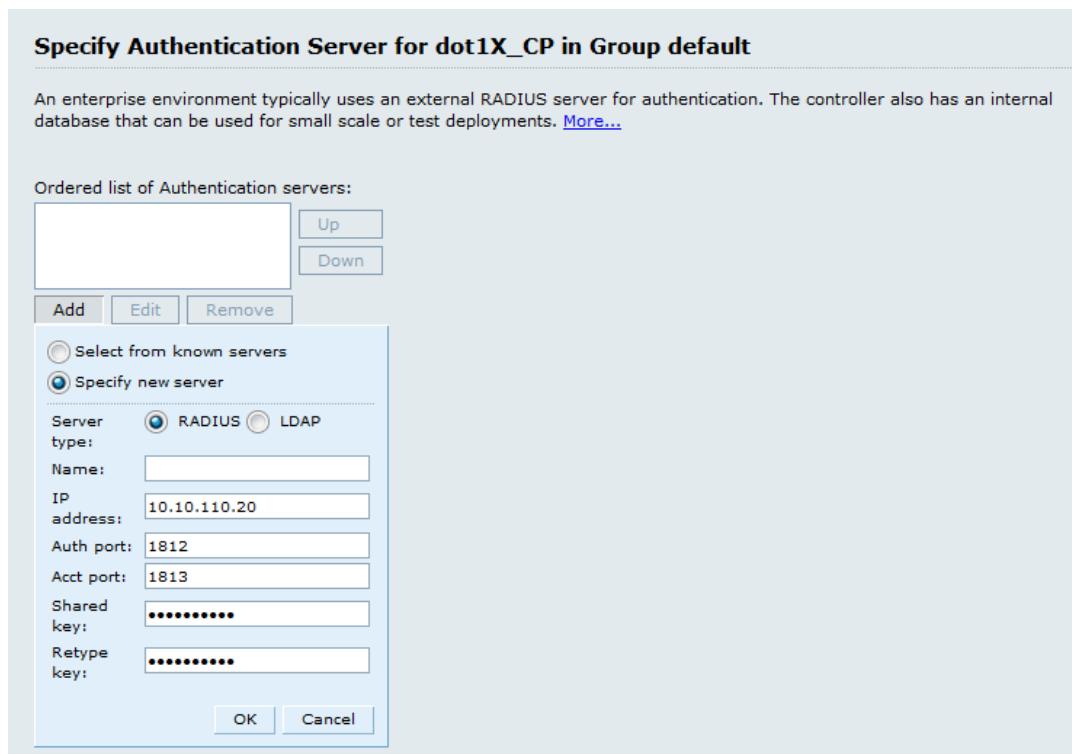
You can either select an existing authentication server or specify a new authentication server.

**Figure 32** Specifying the Authentication Server for the WLAN



11. To specify an existing ClearPass/RADIUS authentication server, click **Add**.
  - a. Choose **Select from known servers**.
  - b. Scroll to select the ClearPass/RADIUS authentication server, then click **OK**.  
The selected server is added to the ordered list of authentication servers.
  - c. Click **Next**.  
The **Configure Role Assignment** screen opens (skip to [Figure 34](#)).
12. To specify a new ClearPass/RADIUS authentication server, click **Add**.
  - a. Choose **Specify new server**.  
The following dialog is displayed:

**Figure 33** Specifying a New Authentication Server



- b. Populate the Authentication Server parameters as described in [Table 11](#).

**Table 11: New SSID Authentication Server Parameters**

Parameter	Action/Description
Server type	1. Choose the default server type: <b>RADIUS</b> .
Name	2. Enter the name of the ClearPass Policy Manager server.
IP address	3. Enter the IP address of the ClearPass Policy Manager server.
Auth port	4. Specify the authentication port on the RADIUS/Policy Manager server. <ul style="list-style-type: none"> <li>● Range: 1 to 65535</li> <li>● Default: 1812</li> </ul>
Acct port	5. Specify the accounting port on the RADIUS/Policy Manager server. <ul style="list-style-type: none"> <li>● Range: 1 to 65535</li> <li>● Default: 1813</li> </ul>
Shared Key	6. Specify the RADIUS Shared Secret for the ClearPass Policy Manager server. <b>NOTE:</b> Make sure that the value of the <b>Key</b> parameter for the RADIUS server configured on the mobility controller is identical to the Shared Key you specify here for the Policy Manager server (see <a href="#">Table 7</a> ).

- c. When finished, click **OK**.

The selected server is added to the ordered list of authentication servers.

- d. Click **Next**.

The **Configure Role Assignment** screen opens.

**Figure 34 Configuring the Role Assignment**

**Configure Role Assignment for dot1x-cp in Group angelapgroup**

After being authenticated, each client is assigned a role, which determines the resources to which the client will have access. You can assign the same role to all clients, or assign server-derived roles based on attributes returned by the authentication server at authentication time. [More...](#)

Default role:

Server-derived roles:

[Show Roles & Policies](#)

- After being authenticated, each client is assigned a role, which determines the network resources that the client will have access to.
- Assigning a role is a method to apply a specific set of policies to that user. If ClearPass does not specify what role to put a user in, that user is assigned the default role.
- You can assign the same default role to all clients, or assign server-based roles based on the attributes returned by the authentication server.

7. Specify the default role, then click **Next**.

The configuration of this Wireless LAN is complete. The **Configuration Summary** page appears, which displays all the settings you configured.

- To print a copy of the WLAN configuration settings, choose **Printable config summary**.

- To see the commands that will be pushed to the mobility controller when the Wireless LAN configuration is applied, choose **Commands to be pushed**.
8. To complete the WLAN wizard and apply the settings you have specified, click **Finish**.  
The settings specified are pushed to the mobility controller. You receive the message:  
*Configuration pushed successfully.*
9. Click **Close**.  
You now have a new set of configurations for the SSID.

## Setting Up the ClearPass Hardware and Virtual Appliances

This section describes the procedures for installing and configuring ClearPass Policy Manager on a hardware appliance, as well as how to install ClearPass on a VMware vSphere Hypervisor host and on a host that runs Microsoft's hypervisor, Hyper-V™.



Due to a negative performance impact when ClearPass 6.7 is installed on a KVM appliance, Aruba will not post the KVM image with this release. For more information, refer to the "6.7.0 Upgrades on KVM Hypervisors are Deferred" section in the ClearPass 6.7 Release Notes.

This section provides the following information:

- [Setting Up the ClearPass Hardware Appliances](#)
- [Using the VMware vSphere Hypervisor Web Client to Install ClearPass on a Virtual Machine](#)
- [Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance](#)

## Setting Up the ClearPass Hardware Appliances

This section documents the procedures for installing and configuring ClearPass on a hardware appliance, as well as how to complete important administrative tasks, such as registering for ClearPass software updates and changing the *admin* password.

This section contains the following information:

- [About the ClearPass Hardware Appliances](#)
- [ClearPass C1000 Hardware Appliance](#)
- [ClearPass C2000 Hardware Appliance](#)
- [ClearPass C3000 Hardware Appliance](#)
- [Before Starting the ClearPass Installation](#)
- [Activating ClearPass](#)
- [Logging in to the ClearPass Hardware Appliance](#)
- [Powering Off the ClearPass Hardware Appliance](#)
- [Resetting the System Passwords to the Factory Defaults](#)

## About the ClearPass Hardware Appliances

Aruba provides three hardware appliance platforms:

- ClearPass Policy Manager C1000
- ClearPass Policy Manager C2000
- ClearPass Policy Manager C3000

**Table 12:** Functional Description of the ClearPass Hardware Appliance Ports

Port	Description
Data port (Gigabit Ethernet)	The Data port (ethernet 1) provides a point of contact for RADIUS, TACACS+, Web authentication, and other dataplane requests. This configuration is optional. If this port is not configured, requests are redirected to the Management port.
iLO port	The iLO (Integrated Lights-Out) port is an Ethernet port that provides out-of-band management facilities. The iLO port makes it possible to perform activities on the ArubaOS switch or an HP server from a remote location. The iLO card has a separate network connection (and its own IP address) to which one can connect via HTTPS.  Available on theClearPass C2000 and C3000 hardware appliances.
Management port (Gigabit Ethernet)	The Management port (ethernet 0) provides access for cluster administration and appliance maintenance using the WebUI, CLI, or internal cluster communication. This configuration is mandatory.
Serial port	The Serial port is used to initially configure the ClearPass hardware appliance using a hard-wired terminal.
SPAN ports	A SPAN (Switched Port Analyzer) port is a method of monitoring network traffic. The switch sends a copy of all network packets seen on one port (which is the <i>monitored</i> or <i>source</i> port) to a destination SPAN port, where the packets can be analyzed.
USB ports	Four USB v2.0 ports are provided on theClearPass C1000 hardware appliance.  Two USB v2.0 ports are provided on the ClearPass C2000 and C3000 hardware appliances.
VGA connector	You can use the VGA Connector to connect the ClearPass hardware appliance to a monitor and keyboard.

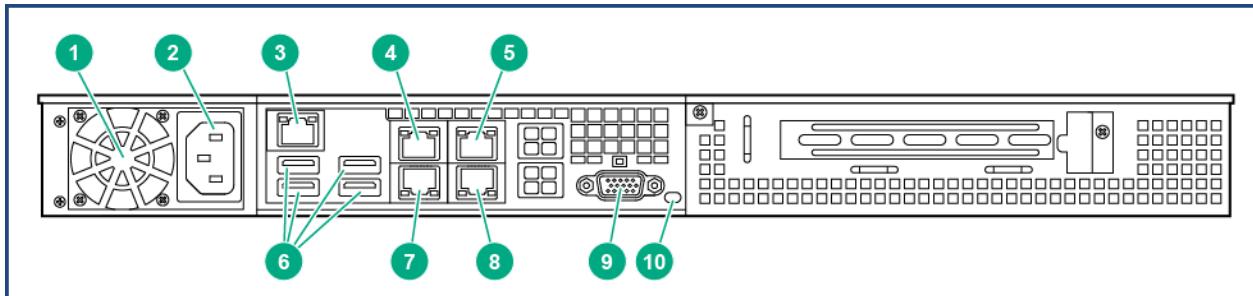
## ClearPass C1000 Hardware Appliance

The ClearPass Policy Manager C1000 hardware appliance (SKU: JZ508A) is a RADIUS/ TACACS+ server that provides advanced policy control for up to 1,000 concurrent sessions.

The ClearPass C1000 appliance has a single 1 TB SATA disk with no RAID disk protection.

[Figure 35](#) shows the ports and components on the rear panel of the ClearPass C1000 hardware appliance. The function of each of these ports and components is described in [Table 12](#).

**Figure 35** Ports and Components on the ClearPass C1000 Hardware Appliance



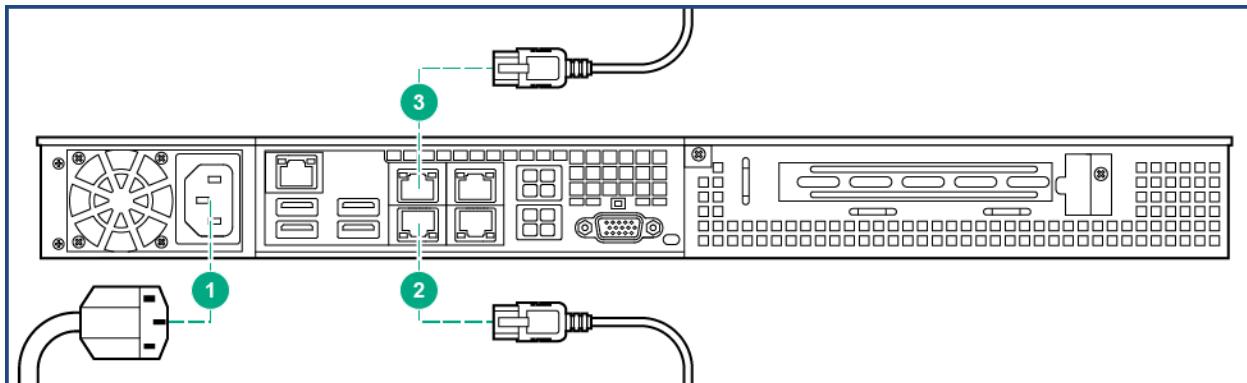
Callout Number	C1000 Port/Component
1	Power supply module fan
2	Power supply AC inlet
3	Serial port
4	Data port (eth1)
5	Port that is optionally available for SPAN-based profiling
6	USB ports (4)
7	Management port (eth0)
8	Port that is optionally available for SPAN-based profiling
9	VGA port
10	Unit Identification (UID) button <b>NOTE:</b> This button is recessed and requires a small tool to access it.

You can also access the ClearPass hardware appliance by connecting a monitor and keyboard to the hardware appliance.

## C1000 Rear-Panel Cabling

Figure 36 illustrates the rear-panel cabling for the ClearPass C1000 hardware appliance.

**Figure 36** C1000 Rear-Panel Cabling



To connect the cables on the ClearPass C1000 hardware appliance:

1. Connect the power cord.
2. Connect the Management port.
3. Optionally connect the Data port.
4. Connect any other required cables.

## Serial Port Cable Signaling and Pinouts

**Table 13:** Serial Port Signaling and Pinouts

Signal	RJ-45Pin	DB-9 Pin	Color
RTS	1	8	GRY
DTR	2	6	BRN
TxD	3	2	YEL
GND	4	5	GRN
GND	5	3	RED
RxD	6	4	BLK
DSR	7	7	ORG
CTS	8	8	BLU

## ClearPass C1000 Hardware Appliance Specifications

[Table 14](#) provides the specifications for the ClearPass Policy Manager C1000 hardware appliance.

**Table 14: ClearPass C1000 Appliance Specifications**

ClearPass C1000 Appliance	Specifications
Hardware Model	Unicom S-1200 R4
CPU	(1) Eight Core 2.4 GHz Atom C2758
Memory	8 GB (2 x 4 GB)
Hard drive storage	<ul style="list-style-type: none"><li>● (1) SATA (7.3K RPM), Serial ATA</li><li>● 1 TB hard drive</li></ul>
Serial Port	Yes: RJ-45
Performance & Scale	Please refer to the <i>ClearPass Scaling &amp; Ordering Guide</i>
Concurrent Sessions	1000
<b>Form Factor</b>	
Rack mount	Included
Dimensions (WxHxD)	17.2" x 1.7" x 11.3"
Weight (max configuration)	8.5 lbs
<b>Power</b>	
Power consumption (maximum)	200 watts
Power supply	Single
AC input voltage	100/240 VAC auto-selecting
AC input frequency	50/60 Hz auto-selecting
<b>Environmental</b>	
Operating temperature	5° C to 35° C (41° F to 95° F)

ClearPass C1000 Appliance	Specifications
Operating vibration	0.26 G at 5 Hz to 200 Hz for 15 minutes
Operating shock	1 shock pulse of 20 G for up to 2.5 ms
Operating altitude	-16 m to 3,048 m (-50 ft to 10,000 ft)

## ClearPass C2000 Hardware Appliance

The ClearPass Policy Manager C2000 hardware appliance (SKU: JZ509A) is a RADIUS/ TACACS+ server that provides advanced policy control for up to 10,000 concurrent sessions.

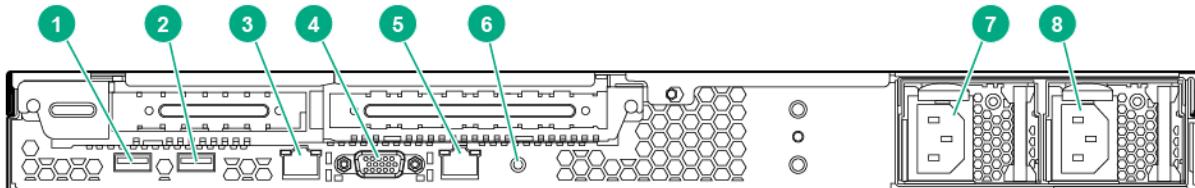
The ClearPass C2000 appliance ships with two x 1TB SATA disk drives. These drives are managed by an LSI RAID-1 controller. The drives are configured as a RAID-1 pair. The LSI controller presents to ClearPass a single virtual 1TB drive, masking the two underlying physical drives.

[Figure 37](#) shows the ports and components on the rear panel of the ClearPass C2000 hardware appliance. The function of each of these ports and components is described in [Table 12](#).



The image of the ClearPass C2000 hardware appliance shown here includes the optional redundant power supply.

**Figure 37** Ports and Components on the ClearPass C2000 Hardware Appliance



Callout Number	C2000 Port/Component
1 and 2	USB ports (2)
3	iLO (Integrated Lights-Out) port and Management port (eth0)
4	VGA Connector
5	Data port (eth1)
6	UID (Unit ID) The UID LED helps you identify and locate a system, especially in high-density rack environments. Additionally, the UID is used to indicate that a critical operation is underway on the host, such as Remote console access or ROM flash. <b>NOTE:</b> This button is recessed and requires a small tool to access it.

Callout Number	C2000 Port/Component
	<p>The "current state" (on or off) of the UID is the last state chosen using one of these methods. If a new state is chosen while the UID is blinking, this new state becomes the current state, and takes effect when the UID stops blinking.</p> <p><b>NOTE:</b> The Unit ID Light web page does not automatically refresh itself if the state of the actual light changes after the page is loaded. To ensure the page accurately reflects the state of the UID Light, click on the Virtual Indicators link to update the page.</p>
7	Power supply AC inlet
8	Optional redundant power supply

You can also access the ClearPass hardware appliance by connecting a monitor and keyboard to the hardware appliance.

[Table 15](#) provides the specifications for the ClearPass C2000 hardware appliance.

**Table 15: ClearPass C2000 Appliance Specifications**

ClearPass C2000 Appliance	Specifications
Hardware Model	HPE DL20 Gen 9
CPU	(1) Xeon 3.5Ghz E3-1240v5 with four cores (8 Threads)
Memory	16 GB
Hard drive storage	<ul style="list-style-type: none"> <li>● (2) SATA (7.2K RPM) 1TB hard drive</li> <li>● RAID-1 controller</li> </ul>
Out-of-Band management	HPE Integrated Lights-Out (iLO) Standard
Serial Port	Yes: Virtual Serial via iLO
Performance & Scale	Please refer to the <i>ClearPass Scaling &amp; Ordering Guide</i>
Concurrent Sessions	10,000
Form Factor	
Rack mount	<ul style="list-style-type: none"> <li>● 1U SFF Easy Install Rail</li> <li>● 1U Cable Management Arm</li> </ul>
Dimensions (WxHxD)	17.11" x 1.70" x 150.5"

ClearPass C2000 Appliance		Specifications
Weight (max configuration)	Up to 19.18 lbs	
<b>Power Specifications</b>		
Power consumption (maximum)	250 watts	
Power supply	HPE 900W AC 240 VDC Power Input FIO Module <b>NOTE:</b> The optional HPE 900W Redundant Power Supply supports 100 VAC to 240 VAC; this power supply also supports 240 VDC.	
Power redundancy	Optional	
AC input voltage	100/240 VAC auto-selecting	
AC input frequency	50/60 Hz auto-selecting	
<b>Environmental Specifications</b>		
Operating temperature	10° C to 35° C (50° F to 95° F)	
Operating vibration	Random vibration at 0.000075 G <sup>2</sup> /Hz, 10Hz to 300Hz, (0.15 G's nominal)	
Operating shock	2 G's	
Operating altitude	3,050 m (10,000 ft)	

## ClearPass C3000 Hardware Appliance

The ClearPass Policy Manager C3000 hardware appliance (SKU: JZ510A) is a RADIUS/ TACACS+ server that provides advanced policy control for up to 50,000 concurrent sessions.

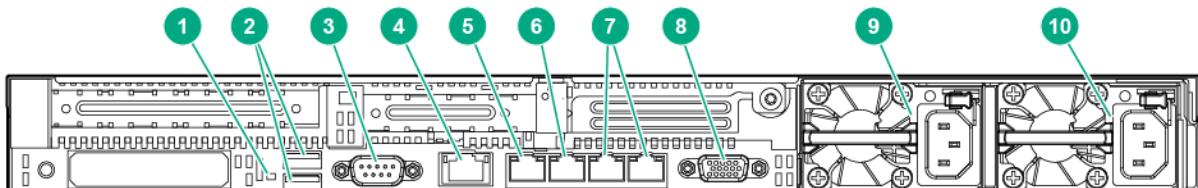
The ClearPass C3000 appliance ships with six Serial-Attach SCSI (SAS) (10K RPM) 600GB Hot-Plug hard drives (RAID-10 controller).

The LSI controller presents to ClearPass a single virtual 1.675 TB drive, masking the underlying two physical drive groups (two groups of two mirrored drives).

[Figure 38](#) shows the ports and components on the rear panel of the ClearPass C3000 hardware appliance. The function of each of these ports and components is described in [Table 12](#).

 The image of the ClearPass C3000 hardware appliance shown here includes the optional redundant power supply.

**Figure 38** Ports and Components on the ClearPass C3000 Hardware Appliance



Callout Number	C3000 Port/Component
1	<p>UID (Unit ID) LED</p> <p>The UID LED helps you identify and locate a system, especially in high-density rack environments. Additionally, the UID is used to indicate that a critical operation is underway on the host, such as Remote console access or ROM flash.</p> <p><b>NOTE:</b> This button is recessed and requires a small tool to access it.</p> <p>The "current state" (on or off) of the UID is the last state chosen using one of these methods. If a new state is chosen while the UID is blinking, this new state becomes the current state, and takes effect when the UID stops blinking.</p> <p><b>NOTE:</b> The Unit ID Light web page does not automatically refresh itself if the state of the actual light changes after the page is loaded. To ensure the page accurately reflects the state of the UID Light, click on the Virtual Indicators link to update the page</p>
2	USB ports (2)
3	Serial port
4	iLO (Integrated Lights-Out) port and Management port (eth0)
5	Management port (eth0)
6	Data port (eth1)
7	Destination SPAN ports (2)
8	VGA Connector
9	Fan and power supply AC inlet
10	Optional redundant fan and power supply

[Table 16](#) provides the specifications for the ClearPass C3000 hardware appliance.

**Table 16: ClearPass C3000 Appliance Specifications**

ClearPass C3000 Appliance		Specifications
Hardware Model		HPE DL360 Gen 9
CPUs		(2) Xeon 2.4GHz E5-2620_V3 with Six Cores (12 Threads)
Memory		64 GB Memory
Hard drive storage		(6) 300GB Serial-Attach SCSI (SAS) (10K RPM) 60 GB Hot-Plug hard drives (RAID-10 controller)
Out-of-Band Management		HPE Integrated Lights-Out (iLO): Advanced
Serial Port		Yes: DB-9
Performance & Scale		Please refer to the <i>ClearPass Scaling &amp; Ordering Guide</i>
Concurrent Sessions		50,000
Form Factor		
Rack mount		<ul style="list-style-type: none"><li>● 1U SFF Easy Install Rail</li><li>● 1U Cable Management Arm</li></ul>
Dimensions (WxHxD)		17.1" x 1.7" x 27.5"
Weight (max configuration)		Up to 33.3 lbs
Power Specifications		
Power supply		HPE 500W Flex Slot Platinum Hot Plug Power Supply
Power Redundancy		Optional
AC input voltage		100/240 VAC auto-selecting
AC input frequency		50/60 Hz auto-selecting
Environmental Specifications		
Operating temperature		10° C to 35° C (50° F to 95° F)

ClearPass C3000 Appliance	Specifications
Operating vibration	Random vibration at 0.000075 G <sup>2</sup> /Hz
Operating shock	2 G's
Operating altitude	3,050 m (10,000 ft)

## Before Starting the ClearPass Installation

Before starting the ClearPass installation and configuration procedures for the hardware appliance, determine the following information for the ClearPass server on your network, note the corresponding values for the parameters listed in [Table 17](#), and keep it for your records:

**Table 17:** *ClearPass Server Configuration Reference*

Required Information	Value for Your Installation
Host name (Policy Manager server)	
Management port IP address	
Management port subnet mask	
Management port gateway	
Data port IP address (optional)	<b>NOTE:</b> Make sure that the Data port IP address is <i>not</i> in the same subnet as the Management port IP address.
Data port subnet mask (optional)	
Data port gateway (optional)	
Primary DNS	
Secondary DNS	
NTP server (optional)	

## Configuring the ClearPass Hardware Appliance

The initial setup dialog starts when you connect a terminal, PC, or laptop running a terminal emulation program to the Serial port on the ClearPass hardware appliance.

To configure the ClearPass Policy Manager hardware appliance:

**1. Connect the Serial port.**

- a. Connect the Serial port to a terminal using a null modem cable.
- b. Power on the hardware appliance.

The hardware appliance is now available for configuration.

**2. Configure the Serial port.**

- **Bit Rate:** 9600
- **Data Bits:** 8
- **Parity:** None
- **Stop Bits:** 1
- **Flow Control:** None

**3. Log in.**

Use the following preconfigured credentials to log in to the hardware appliance.

(You will create a unique appliance/cluster administration password in Step 5.)

- login: **appadmin**
- password: **eTIPS123**

This initiates the Policy Manager configuration wizard.

**4. Configure the ClearPass hardware appliance.**

Follow the prompts, replacing the placeholder entries in the following illustration with the information you entered in [Table 17](#):

- Enter hostname:
- Enter Management Port IP Address:
- Enter Management Port Subnet Mask:
- Enter Management Port Gateway:
- Enter Data Port IP Address:
- Enter Data Port Subnet Mask:
- Enter Data Port Gateway:
- Enter Primary DNS:
- Enter Secondary DNS:

**5. Specify the cluster password.**



Setting the cluster password also changes the password for the CLI user **appadmin**, as well as the Administrative user **admin**. If you want the **admin** password to be unique, see [Changing the Administration Password on page 74](#).

- a. Enter any string with a minimum of six characters, then you are prompted to confirm the cluster password.
- b. After this configuration is applied, use this new password for cluster administration and management of the ClearPass virtual appliance.

**6. Configure the system date and time.**

- a. Follow the prompts to configure the system date and time.

- b. To set the date and time by configuring the NTP server, use the primary and secondary NTP server information you entered in [Table 17](#).

## 7. Apply the configuration.

- a. To apply the configuration, press **Y**.
  - To restart the configuration procedure, press **N**.
  - To quit the setup process, press **Q**.

Configuration on the hardware appliance console is now complete. The next task is to activate the ClearPass product.

## Activating ClearPass

To activate ClearPass Policy Manager and apply the ClearPass license:

1. After the configuration has been applied at the virtual appliance console, open a web browser and navigate to the ClearPass Policy Manager server:

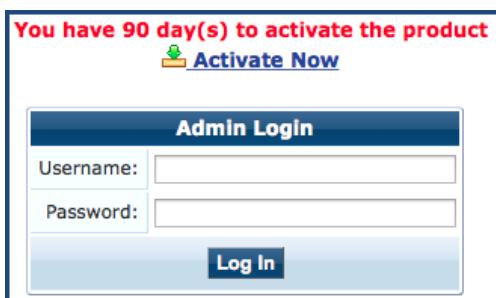
**<https://x.x.x.x/tips/>**

where **x.x.x.x** is the IP address of the management interface defined for the ClearPass server as listed in [Table 17](#).

2. Accept any security warnings from your browser regarding the self-signed SSL certificate, which comes installed in ClearPass by default.

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 39** Activating ClearPass

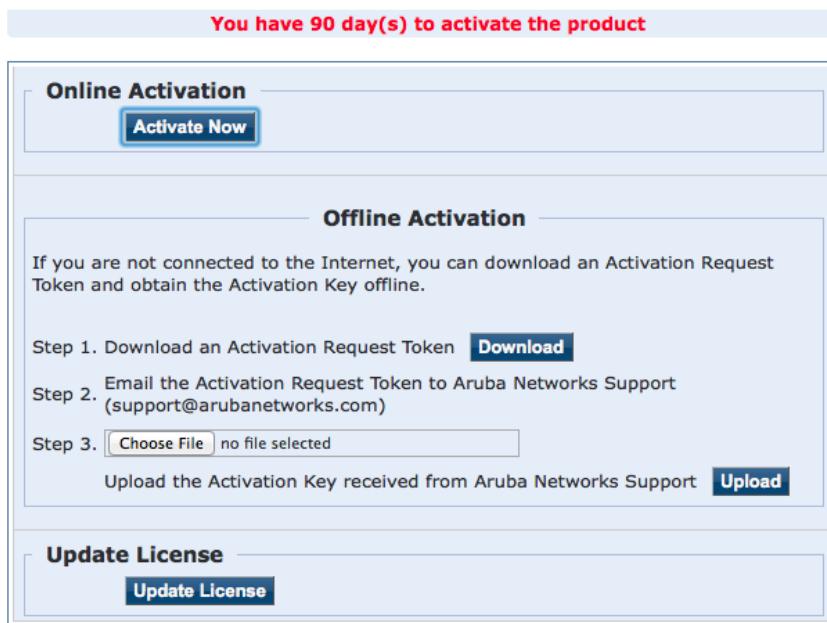


3. To activate ClearPass on this hardware appliance, click **Activate Now**.

When you click **Activate Now**, ClearPass Policy Manager attempts to activate the product over the Internet with Aruba Networks license activation servers.

If the ClearPass Policy Manager hardware appliance does not have Internet access, you can perform the product activation offline by following the steps for offline activation presented in the **Offline Activation** section shown in [Figure 40](#).

**Figure 40** Performing Offline Activation



4. If the ClearPass server is connected to the Internet, click the **Activate Now** button.

You receive the message, "*Product has been successfully activated*" and the **Admin Login** dialog is displayed.

## Logging in to the ClearPass Hardware Appliance

After a successful activation, the **Admin Login** dialog appears.

**Figure 41** Logging in to the ClearPass Hardware Appliance

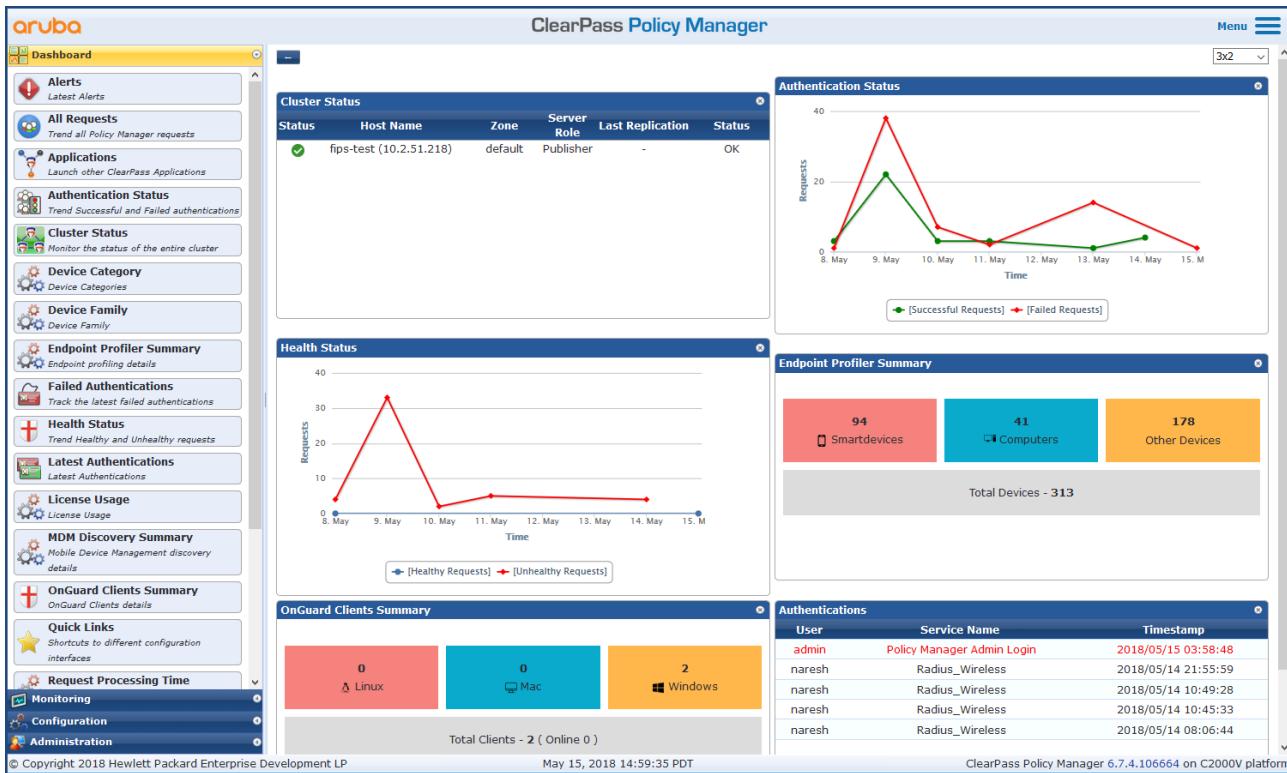
The Admin Login dialog box contains the following fields and button:

- Username:** admin
- Password:** **.....**
- Log In**

1. Log in to the ClearPass hardware appliance with the following credentials:
  - **Username:** admin
  - **Password:** Enter the cluster password defined in [Configuring the ClearPass Hardware Appliance](#).
2. Click **Log In**.

The ClearPass Policy Manager Landing Page opens.

**Figure 42** ClearPass Policy Manager Landing Page



## Changing the Administration Password

When the cluster password for this ClearPass server is set upon initial configuration, the administration password is also set to the same password (see [Configuring the ClearPass Hardware Appliance](#)).

If you wish to assign a unique **admin** password, use this procedure to change it.

To change the administration password:

1. In ClearPass, navigate to **Administration > Users and Privileges > Admin Users**.

The **Admin Users** page opens.

**Figure 43** Admin Users Page

The Admin Users page displays the following table:

#	User ID	Name	Privilege Level	Status
1.	<input checked="" type="checkbox"/> admin	Super Admin	Super Administrator	Enabled
2.	<input type="checkbox"/> apiadmin	API Admin	API Administrator	Enabled

2. Select the appropriate **admin** user.

The **Edit Admin User** dialog opens.

**Figure 44** Changing the Administration Password

Edit Admin User	
User ID:	admin
Name:	Super Admin
Password:	[REDACTED]
Verify Password:	[REDACTED]
Enable User:	<input checked="" type="checkbox"/> (Check to enable user)
Privilege Level	Super Administrator
<b>Save</b> <b>Cancel</b>	

3. Change the administration password, verify the new password, then click **Save**.

## Powering Off the ClearPass Hardware Appliance

This procedure gracefully shuts down the hardware appliance without having to log in.

To power off the ClearPass hardware appliance:

1. Connect to the CLI from the serial console using the serial port.
2. Enter the following commands:
  - login: poweroff
  - password: poweroffThe ClearPass hardware appliance shuts down.

You can also power off from the WebUI and the appadmin prompt.



## Resetting the System Passwords to the Factory Defaults

To reset the system account passwords in Policy Manager to the factory defaults, you must first generate a password recovery key, then log in as the *apprecovery* user to reset the system account passwords.

### Generating the Password Recovery Key

To generate the password recovery key:

1. If you are employing a hardware connection, connect to the ClearPass Policy Manager hardware appliance using the serial port (using any terminal program). See [Configuring the ClearPass Hardware Appliance](#) for details.
  - a. If you are employing a virtual appliance, use the VMware console or the Hyper-V hypervisor (see for details).
2. Reboot the system using the **restart** command.
3. After the system reboots, the following prompt is displayed for ten seconds:  
Generate support keys? [y/n] :
4. At the prompt, enter **y**.

The system prompts you with the following choices:

```
Please select a support key generation option.  
1) Generate password recovery key
```

- 2) Generate a support key
  - 3) Generate password recovery and support keys
- Enter the option or press any key to quit.
5. To generate a password recovery key, select option **1**.
  6. After the password recovery key is generated, email the key to Aruba Technical Support.  
A unique password is dynamically generated from the recovery key and emailed to you.

## **Resetting the System Account Passwords to the Factory Defaults**

To reset the administrator password:

1. Log in as the **apprecovery** user with the password recovery key provided by Aruba Technical Support.
2. Enter the following command at the command prompt:

```
[apprecovery] app reset-passwd
*****
* WARNING: This command will reset the system account *
* passwords to factory default values *
*****
Are you sure you want to continue? [y/n]: y
INFO - Password changed on local node
INFO - System account passwords have been reset to factory default values
```

3. To reset the system account passwords to the factory default values, enter **y**.

You can now log in with the new administrator password emailed to you by Aruba Technical Support.

## **Using the VMware vSphere Hypervisor Web Client to Install ClearPass on a Virtual Machine**

This section documents the procedures for using the VMware vSphere® Web Client to install ClearPass on a vSphere Hypervisor (ESXi) host, as well as completing important administrative tasks, such as registering for ClearPass software updates and changing the admin password.

This section contains the following information:

- [Introduction](#)
- [Virtual Appliance Platforms](#)
- [Before Starting the ClearPass Installation](#)
- [vSphere Web Client ClearPass Installation Overview](#)
- [ClearPass VMware Virtual Appliance Installation Setup](#)
- [Adding a Virtual Hard Disk](#)
- [Launching the ClearPass Virtual Appliance](#)
- [Completing the Virtual Appliance Setup](#)
- [Initial Login and Activation of the ClearPass Platform License](#)
- [Logging in to the ClearPass Virtual Appliance](#)
- [About Software Updates](#)
- [Software Updates Page](#)
- [Changing the Administration Password](#)

- [Powering Off the ClearPass Virtual Appliance](#)

## Introduction

The VMware vSphere® Web Client enables you to connect to a vCenter Server system to manage an ESX host through a browser.

This section assumes that the VMware vSphere Web Client has been installed. For information about installing and starting the vSphere Web Client, go to [VMware Documentation](#).

## Meeting the Recommended vSphere HypervisorServer Specifications

Please carefully review all virtual appliance requirements, including functional IOP ratings, and verify that your system meets these requirements. These recommendations supersede earlier requirements that were published for ClearPass Policy Manager 6.7 installations.

Virtual appliance recommendations are adjusted to align with the requirements for ClearPass hardware appliances. If you do not have the virtual appliance resources to support a full workload, you should consider ordering the ClearPass Policy Manager hardware appliance.

Be sure that your system meets the recommended specifications required for the Policy Manager virtual appliance.

### Supplemental Storage/Hard Disk Requirement

All VMware vSphere Hypervisor virtual machines use hardware version 8.

ClearPass VMware ships with a 30 GB hard disk volume. This must be supplemented with additional storage/hard disk by adding a virtual hard disk (see [Adding a Virtual Hard Disk on page 82](#) for details). The additional space required depends on the ClearPass virtual appliance version.

### Processing and Memory Requirements

To ensure scalability, dedicate or reserve the processing and memory to the ClearPass VM instance. You must also ensure that the disk subsystem can maintain the IOPs (I/O operations per second) throughput as detailed below.

#### ClearPass Server I/O Rate

Most virtualized environments use a shared disk subsystem, assuming that each application will have bursts of I/O without a sustained high I/O throughput. ClearPass Policy Manager requires a continuous sustained high data-I/O rate.



---

For the latest information on the supported hypervisors and virtual hardware requirements, refer to the Release Notes in the appropriate version folder under **Support Center > Documentation > Software User & Reference Guides > ClearPass > Release Notes**.

---

### Supported Hypervisors

ClearPass supports the following hypervisors:

Hypervisor	Supported Versions
VMware vSphere Hypervisor (ESXi)	<ul style="list-style-type: none"> <li>5.5</li> <li>6.0</li> <li>6.5 U1</li> </ul>
Microsoft Hyper-V	<ul style="list-style-type: none"> <li>Windows Server 2012 R2</li> <li>Windows Server 2016</li> <li>Windows Server 2012 R2 with Hyper-V</li> <li>Windows Server 2016 with Hyper-V</li> </ul>

## Virtual Appliance Platforms

Aruba provides three virtual appliance platforms, plus an evaluation platform:

- ClearPassPolicy Manager C1000V
- ClearPassPolicy Manager C2000V
- ClearPassPolicy Manager C3000V
- ClearPassPolicy Manager CLABV

## Before Starting the ClearPass Installation

Before starting the ClearPass installation and configuration procedures for the virtual appliance, determine the following ClearPass server information on your network, note the corresponding values for the parameters listed in [Table 18](#), and keep it for your records:

**Table 18: ClearPass Server Configuration Information**

Required Information	Value for Your Installation
Host name (Policy Manager server)	
Management interface IP address	
Management interface subnet mask	
Management interface gateway	
Data port IP address (optional)	<b>NOTE:</b> Make sure that the Data interface IP address is <i>not</i> in the same subnet as the Management interface IP address.
Data interface subnet mask (optional)	

Required Information	Value for Your Installation
Data interface gateway (optional)	
Primary DNS	
Secondary DNS	
NTP server (optional)	

## vSphere Web Client ClearPass Installation Overview

ClearPass VMware software packages are distributed as Zip files.

The process of installing the ClearPass Policy Manager virtual appliance on a host that runs VMware vSphere Web Client consists of four stages:

1. Download the vSphere Hypervisor software image from the **Download Software > ClearPass > Policy Manager > Current Release > ESXi** folder on the Aruba Support Center and unzip it to a folder on your server to extract the files.
2. Follow the steps in the OVF wizard to deploy the OVF file, **but do not power on yet.**

 There is only one OVF file with all the variant types and sizes selectable when the virtual appliance boots.
3. Add a new hard disk, based on the requirements for your type of virtual machine.
4. Power on and configure the virtual appliance.

## ClearPass VMware Virtual Appliance Installation Setup

To set up the ClearPass Policy Manager virtual appliance installation on a host that runs VMware vSphere Web Client consists of four stages:

1. Download the Release Notes for the version of ClearPass that you want to install as a virtual appliance.
 

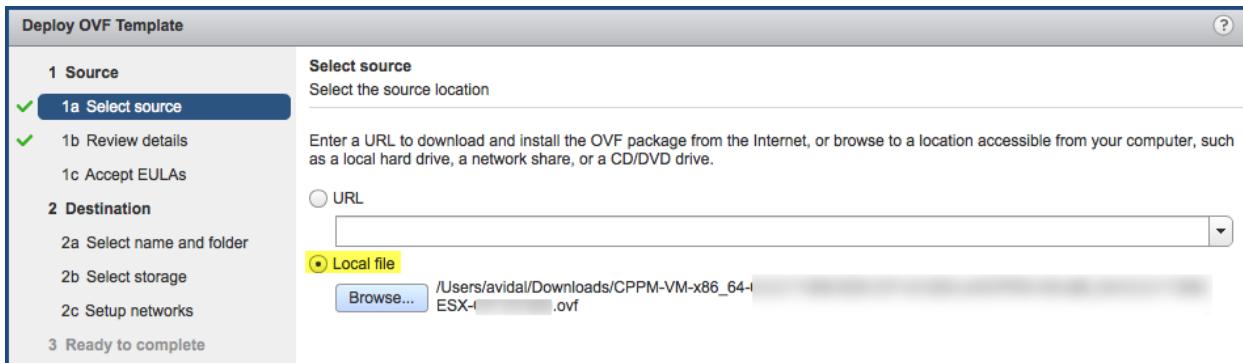
 Release Notes are available in the appropriate version folder under **Aruba Support Center > Documentation > Software User & Reference Guides > ClearPass > Release Notes.**
2. Then check the recommended virtual hardware specifications and verify that your system meets those requirements.
3. Start the VMware vSphere Web Client.
4. Extract the files into a folder on your desktop.
5. Using either the VMware vSphere Web Client or the standard vSphere Client, deploy the Open Virtualization Format (OVF) template that was downloaded and extracted in **Steps 3 and 4.**

The Deploy OVF Template opens.

 If you are not using the vSphere Web Client or the standard vSphere Client, follow the instructions for your method of deploying the OVF file.

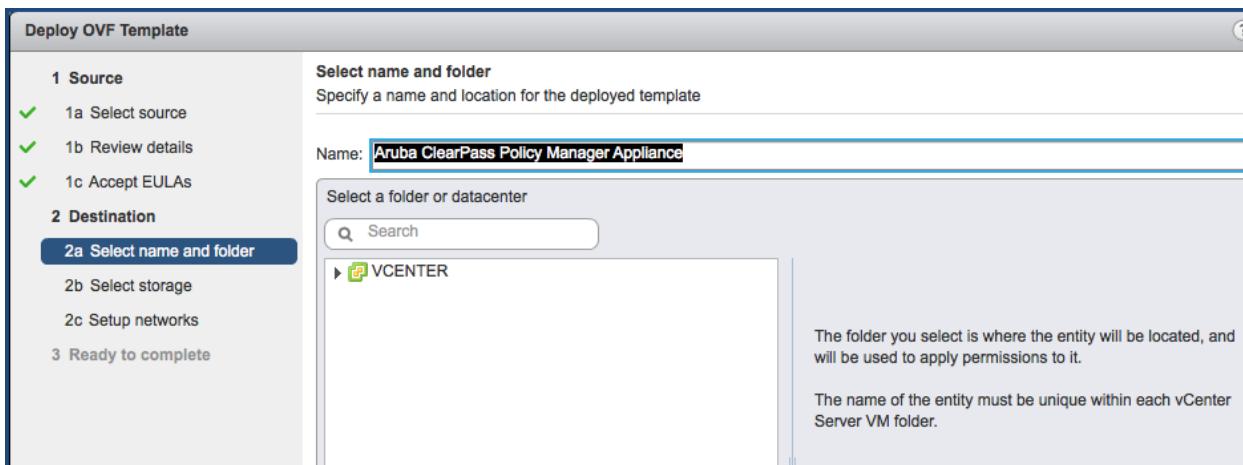


**Figure 45 Deploy OVF Template: Selecting the Source Location**



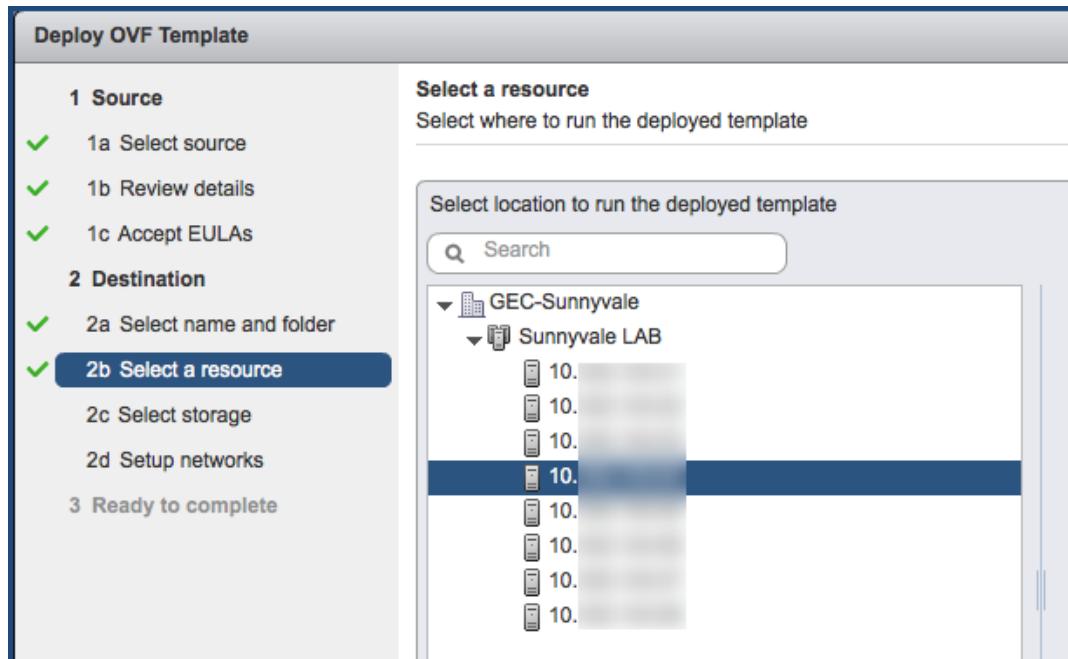
6. Select **Local File**, then click **Browse**.
7. Navigate to the folder where you extracted the files, then click **Next**.  
The **Review Details** screen opens.
8. Review the information presented, then click **Next**.  
The **Accept EULAs** screen opens.
9. Read the End User License Agreements (EULA) and click **Accept**, then click **Next**.  
The **Select Name and Folder** screen opens.

**Figure 46 Selecting the Name and Location for the Deployed Template**



10. In the **Select Name and Folder** dialog:
    - The name of the template is set by default to *ClearPass Policy Manager Appliance*.
    - a. Change the name to the desired virtual appliance name.
    - b. Select the virtual appliance folder or data center where you want to deploy the ClearPass OVF file, then click **Next**.
- The **Select a Resource** screen opens.

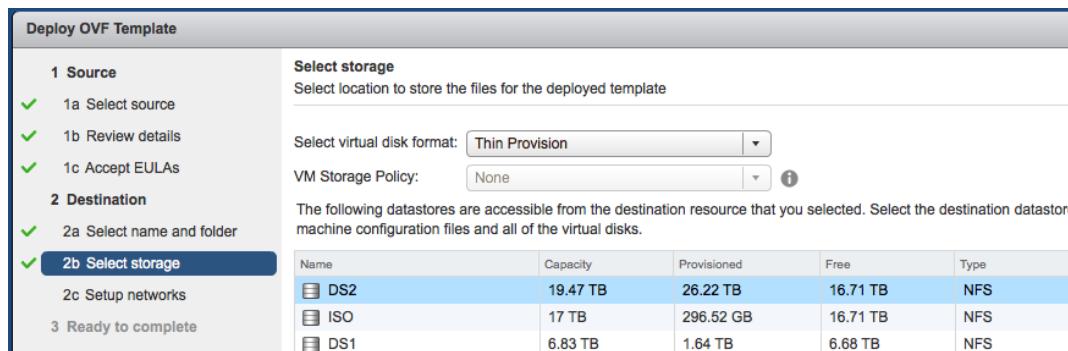
**Figure 47** Selecting a Resource



11. If required, choose the VMware host where ClearPass will be deployed, then click **Next**.

The **Select Storage** screen opens.

**Figure 48** Selecting the Location to Store the Files



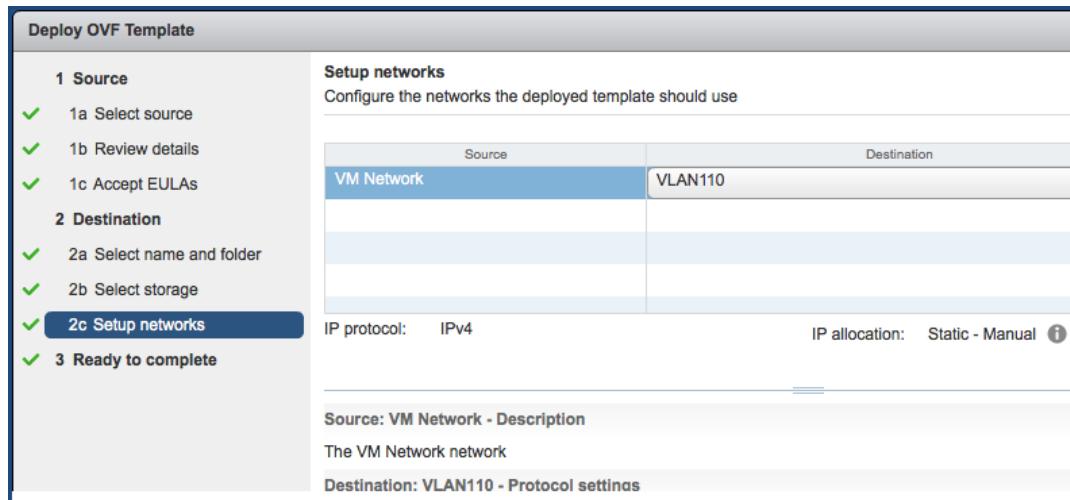
12. Choose the virtual disk format and data store for the ClearPass virtual appliance, then click **Next**.

The virtual disk format specified in [Figure 48](#) is **Thin Provision**. In a production environment, to ensure that the virtual appliance will not run out of disk space, Aruba recommends using the **Thick Lazy Zeroed** virtual disk format.



The **Setup Networks** screen opens.

**Figure 49** Configuring the Networks for VM Deployment



13. Specify the virtual network where ClearPass will reside, then click **Next**.

The **Ready to Complete** screen opens, which displays all the settings you chose for this OVF file deployment.

14. Review the settings for accuracy, and make any changes if necessary, then click **Finish**.

The OVF file is deployed in the selected network.

## Adding a Virtual Hard Disk

After the OVF file has been deployed and before you power on, you must add a virtual hard disk to the virtual machine hardware and make sure that the network adapters are assigned correctly.

1. From the ClearPass Policy Manager Appliance, select the **Summary** tab.

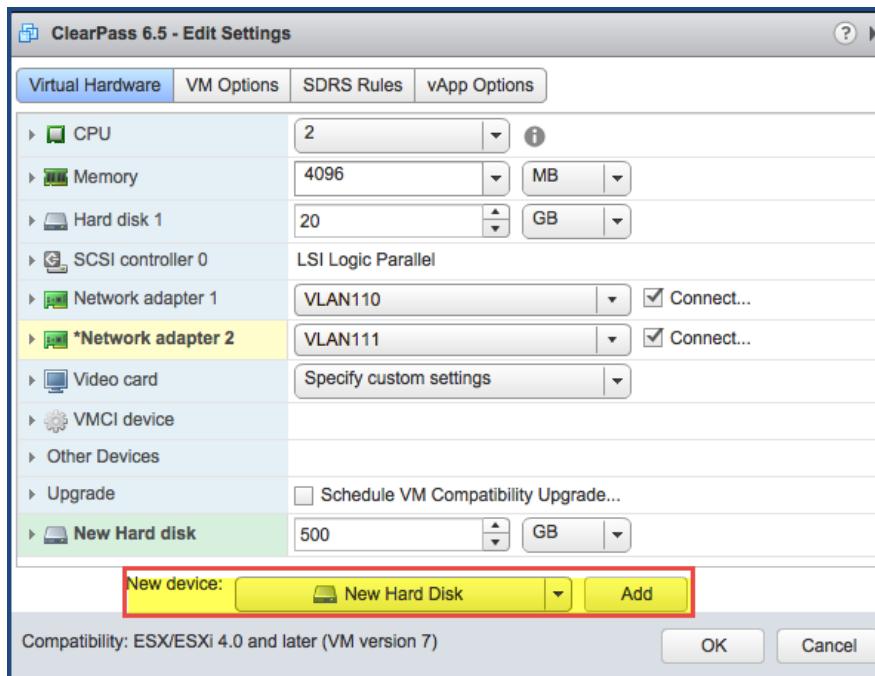
**Figure 50** Virtual Appliance Summary Tab

The screenshot shows the Aruba ClearPass Policy Manager Appliance summary tab. It includes fields for Guest OS (CentOS 4/5/6 (64-bit)), Compatibility (ESX/ESXi 4.0 and later (VM version 7)), and VMware Tools (Not running, version:9344 (Current)). The VM is currently Powered Off. The VM Hardware section lists CPU (2 CPU(s), 0 MHz used), Memory (4096 MB, 0 MB used), Hard disk 1 (20 GB), Network adapter 1 (VLAN110, disconnected), Network adapter 2 (VLAN111, disconnected), Video card (4 MB), and Other (Additional Hardware). The VM Storage Policies section lists VM Storage Policies, VM Storage Policy Compliance, and Last Checked Date. The Tags section indicates 'This list is empty.' A red box highlights the 'Edit Settings.' button at the bottom right.

2. Click **Edit Settings**.

The **Edit Settings** dialog opens.

**Figure 51** Editing the Virtual Machine Settings

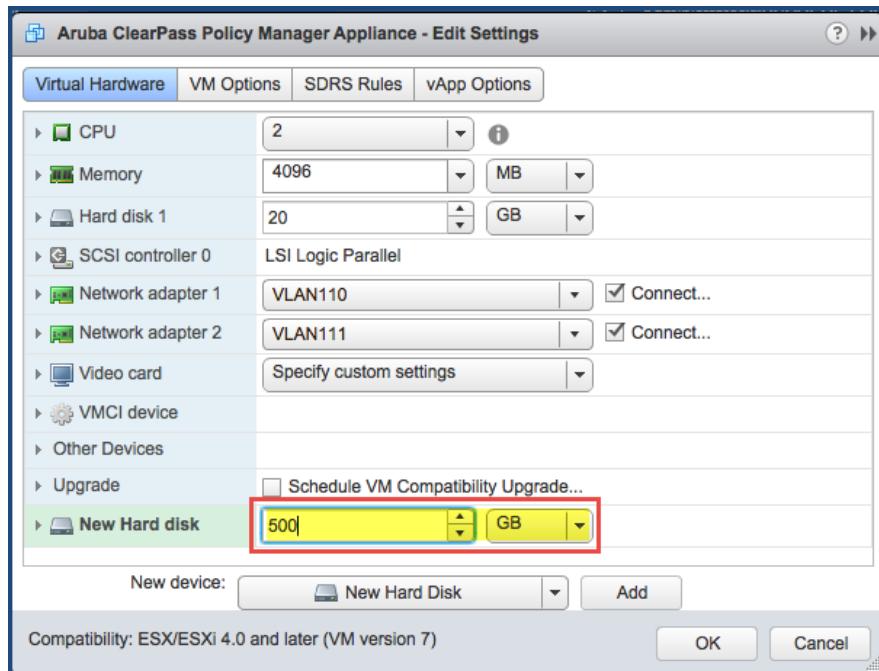


3. Add a new virtual hard disk:

- Consult the ClearPass Policy Manager Release Notes for determining the correct size of the virtual hard disk to add to your ClearPass virtual appliance.
- From the **New Device** drop-down, select **New Hard Disk**.
- Click **Add**.

The **Virtual Hardware** dialog opens.

**Figure 52 Specifying the Size of the New Hard Disk**



- d. Specify the size of the new hard disk (as shown in [Figure 52](#)), then click **OK**.

For the latest test information on the recommended disk sizes for a virtual hard disk, refer to the Release Notes in the appropriate version folders under **Aruba Support Center > Documentation > Software User & Reference Guides > ClearPass > Release Notes**.



4. Make sure that the network adapters are assigned correctly:

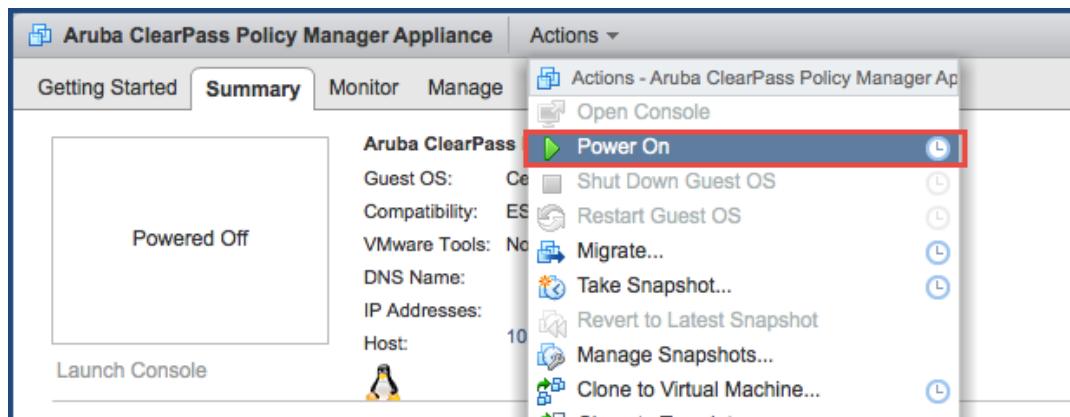
- Network adapter 1: Management port**
- Network adapter 2: Data port**
- Click **OK**.

## Launching the ClearPass Virtual Appliance

To launch the ClearPass virtual appliance:

1. To power on the virtual appliance, from the ClearPass Policy Manager Appliance, choose **Actions > Power On**.

**Figure 53 Powering on the Virtual Machine**



The virtual appliance is now powered on.

2. To launch the VM console, choose **Actions** > **Launch Console**.

The initial virtual machine console screen is displayed. At the bottom of the console screen is the following prompt:

*Enter 'y' or 'Y' to proceed:*

3. To proceed, enter **y**.

ClearPass setup and installation begins.

The console screen appears.

4. Enter the **number** for the appropriate appliance type (do not enter the appliance model itself).

For example, to specify the **C3000V** appliance, you would enter the number **4**. Options include:

- **1) CLABV**
- **2) C1000V**
- **3) C2000V**
- **4) C3000V**

The system requirements are displayed for the appliance model you entered, along with your current system configuration.

5. Compare these to make sure your system meets the new system requirements.

6. When you have verified that your system meets the new requirements, press **y**.

ClearPass will reboot at least once.

Two console screens appear sequentially, which indicate that first the ClearPass Installer reboots, then the virtual appliance reboots.

When the rebooting process is complete, the ClearPass virtual appliance is configured, and it will power on and boot up within a couple of minutes. The whole process, from deploying the OVF image to the login banner screen, typically takes between 30 and 40 minutes.

7. After the ClearPass virtual appliance launches correctly, the virtual machine login banner is displayed.

8. Proceed to the next section, [Completing the Virtual Appliance Setup](#).

## Completing the Virtual Appliance Setup

To complete the virtual appliance setup:

1. Refer to and note the required ClearPass server configuration information listed in [Table 18](#).

2. **Log in to the virtual appliance** using the following preconfigured credentials:

- login: **appadmin**
- password: **<password>**

This initiates the Policy Manager Configuration wizard.

3. **Configure the ClearPass virtual appliance.**

Follow the prompts, replacing the placeholder entries in the following illustration with the information you entered in [Table 18](#).

- Enter hostname:
- Enter Management Port IP Address:
- Enter Management Port Subnet Mask:
- Enter Management Port Gateway:
- Enter Data Port IP Address:
- Enter Data Port Subnet Mask:
- Enter Data Port Gateway:



- Enter Primary DNS:
- Enter Secondary DNS:

#### 4. Specify the cluster password.

Setting the cluster password also changes the password for the CLI user **appadmin**, as well as the Administrative user **admin**. If you want the **admin** password to be unique, see [Changing the Administration Password on page 93](#).

- a. Enter any string with a minimum of six characters, then you are prompted to confirm the cluster password.
- b. After this configuration is applied, use this new password for cluster administration and management of the ClearPass virtual appliance.

#### 5. Configure the system date and time.

- a. Follow the prompts to configure the system date and time.
- b. To set the date and time by configuring the NTP server, use the primary and secondary NTP server information you entered in [Table 18](#).

#### 6. Apply the configuration.

Follow the prompts and do one of the following:

- a. To apply the configuration, press **Y**.
  - To restart the configuration procedure, press **N**.
  - To quit the setup process, press **Q**.

Configuration on the virtual appliance console is now complete. The next task is to activate the ClearPass license, which is described in the next section.

### Initial Login and Activation of the ClearPass Platform License

Upon initial login to a ClearPass 6.7 server, you are prompted to enter the ClearPass Platform License Key. The ClearPass 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.

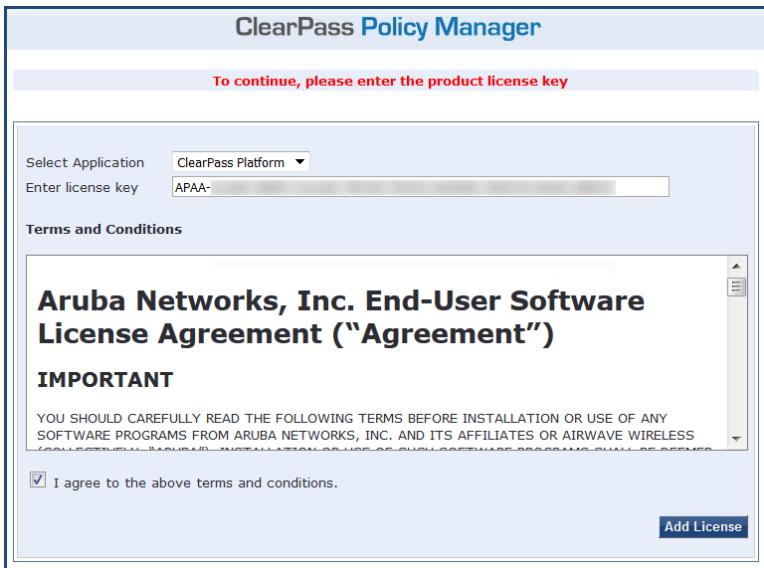
The ClearPass Platform License is the base-level license. Each ClearPass server has one ClearPass Platform License for the physical hardware. Virtual devices have a ClearPass Platform License as well on a per-expected device level.

To specify the ClearPass Platform license upon initial login:

1. After the configuration has been applied at the virtual appliance console, open a web browser and go to the management interface of ClearPassPolicy Manager: <https://x.x.x.x/tips/>, where **x.x.x.x** is the IP address of the management interface defined for the ClearPass server in [Table 18](#).
2. Log in to the ClearPass 6.7 server.
3. Accept any security warnings from your browser regarding the self-signed SSL certificate, which comes installed in ClearPass by default.

The ClearPass Policy Manager End-User Software License Agreement dialog is displayed.

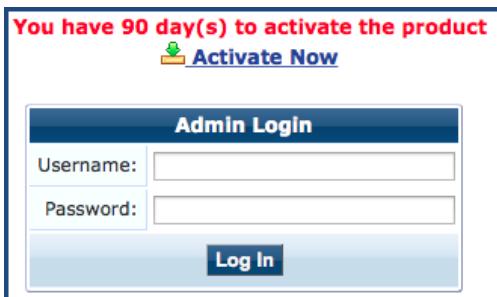
**Figure 54** Entering the ClearPass Platform License Key



4. Enter the ClearPass Platform License Key.
5. Click the check box for **I agree to the above terms and conditions.**  
The **Add License** button is now enabled.
6. Click **Add License**.

Upon successfully entering the Platform License Key, 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 55** Activating ClearPass



7. To activate ClearPass on this virtual appliance, click **Activate Now**.

When you click **Activate Now**, ClearPassPolicy Manager attempts to activate the license over the Internet with Aruba Networks license activation servers.

If the ClearPassPolicy Manager virtual appliance does not have Internet access, you can perform the license activation offline by following the steps for offline activation presented in the **Offline Activation** section shown in [Figure 56](#).

**Figure 56** Performing Offline Activation

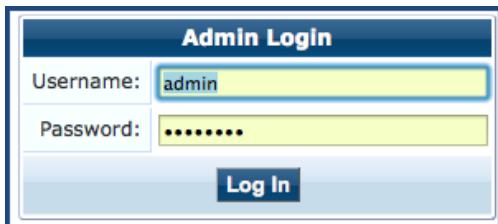


After successfully activating ClearPass online, you will see a message above the **Admin Login** screen indicating that the product has been successfully activated.

## Logging in to the ClearPass Virtual Appliance

After a successful activation, the **Admin Login** dialog appears.

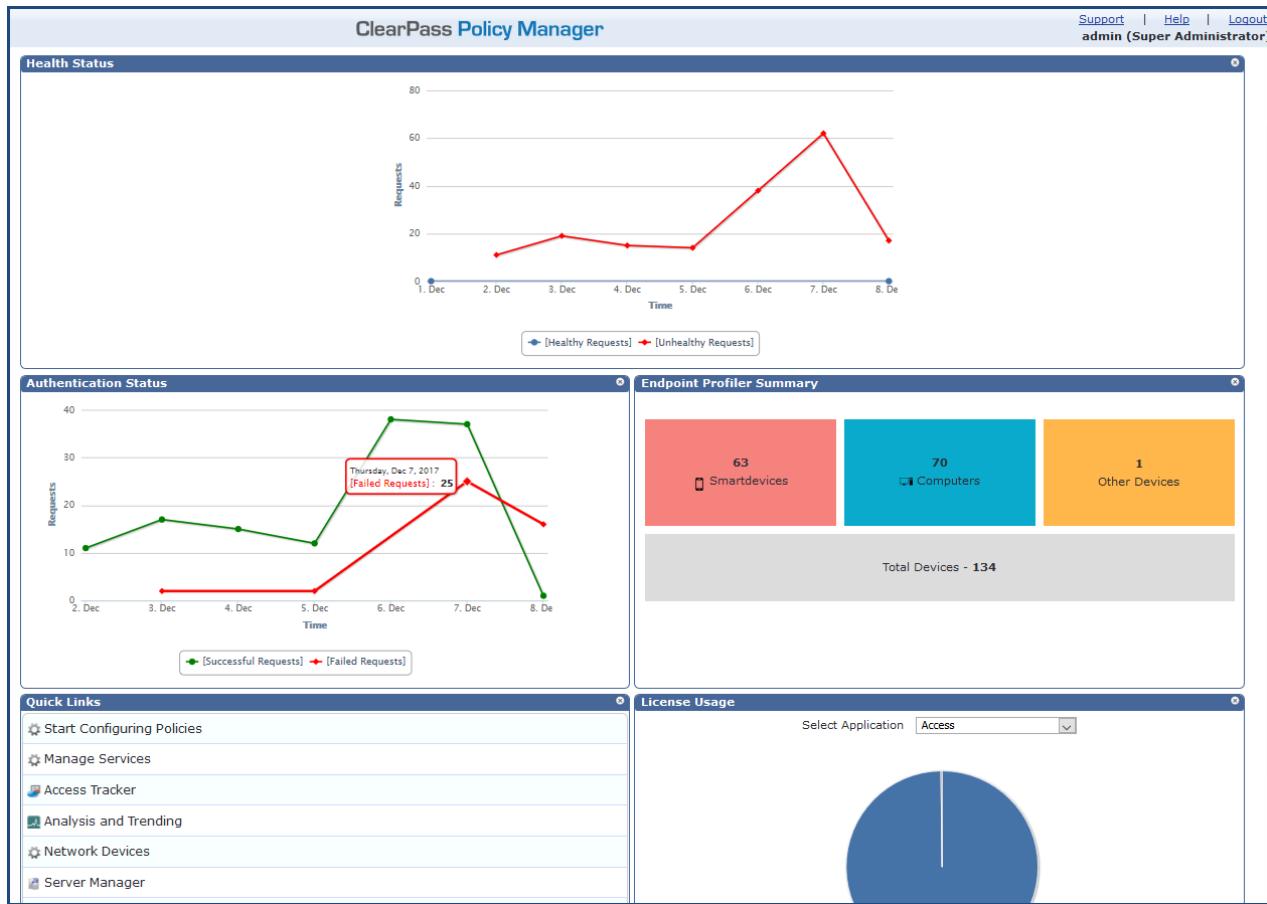
**Figure 57** Logging in to the ClearPass Virtual Appliance



1. Log in to the ClearPass virtual appliance with the following credentials:
  - **Username:** admin
  - **Password:** Enter the cluster password defined in [Completing the Virtual Appliance Setup on page 85](#).
2. Click **Log In**.

The ClearPass Policy Manager opens.

**Figure 58** ClearPass Policy Manager Landing Page



## About Software Updates

This section describes the ClearPass server software update process.

ClearPass 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 59](#) displays the **Software Updates** page:

**Figure 59** Software Updates Page

The screenshot shows the 'Software Updates' page under 'Agents and Software Updates'. It includes sections for 'HPE Passport Credentials' (Username: HPEpassport@hpe.com, Password: masked), 'Posture & Profile Data Updates' (listing Posture Signature, Windows Hotfixes, and Endpoint Profile updates), and 'Firmware & Patch Updates' (listing patches for ClearPass OnGuard Engine and Guest Skin). Buttons for 'Import Updates' and 'Check Status Now' are visible.

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
Posture Signature Updates*	1.49236	2017/11/01 13:30:05	Online	2017/11/01 22:00:03	Updated 1 day ago
Windows Hotfixes Updates*	1.2181	2017/10/31 16:50:27	Online	2017/11/01 22:00:05	Updated 1 day ago
Endpoint Profile Fingerprints*	2.545	2017/10/24 11:15:29	File	2017/11/01 15:06:21	Updated 1 day ago

Update Type	Name	Version	Size (MB)	Update Released	Last Checked	Status	Delete
Patch	6.7.0.100772*	-	0.0040	2017/11/15	2017/11/02 16:10:22	<b>Download</b>	-
Patch	ClearPass OnGuard Engine 1.0 Update 1†‡	1.0.0.101255	62.7049	2017/10/30	2017/11/02 16:10:22	<b>Installed</b>	-
Guest Skin	Fidelity Investments Skin	0.1.6-0	0.6084	2013/09/09	2017/11/02 16:10:22	<b>Download</b>	-

The following describes the **Software Updates** parameters:

**Table 19: Software Updates Page Parameters**

Parameter	Action/Description
<b>HPE Passport Credentials</b>	
HPE Passport Credentials	<p>Enter the <b>HPE Passport Credentials</b> provided to you.</p> <p>This text box is enabled only on a Publisher node.</p> <p>The first time the HPE Passport Credentials are saved, the ClearPass server performs the following operations:</p> <ul style="list-style-type: none"> <li>Contacts the Webservice server to download the latest Posture &amp; Profile Data updates (depending on the Cluster-Wide Parameter settings for those parameters).</li> <li>Checks for any available firmware and patch updates.</li> </ul>
<b>Posture &amp; Profile Data Updates</b>	
Import Updates	<p>To download the Posture and Profile Data Updates to the client (for example, a Windows laptop):</p> <ol style="list-style-type: none"> <li>From the client device, log in to the <a href="#">Aruba Support Center</a>.</li> <li>Select the <b>Download Software</b> tab, then navigate to <b>ClearPass &gt; Tools &gt; Posture &amp; Profile Data Updates</b>.</li> <li>Click the desired update(s) (which are in zip file format) and save the file.</li> <li>From ClearPass, click the <b>Posture and Profile Data Updates &gt; Import Updates</b> button to import the downloaded file into ClearPass.</li> </ol> <p><b>NOTE:</b> In a ClearPass cluster, the <b>Import Updates</b> option is available on the Publisher node only.</p> <p>By default, updates for <b>Posture Signature</b>, <b>Windows Hotfixes</b>, and <b>Endpoint Profile Fingerprints</b> are <i>not</i> automatically downloaded and installed. To set these updates to be automatic, you must set the following Cluster-Wide Parameters to <b>TRUE</b>:</p> <ul style="list-style-type: none"> <li><b>Automatically download Posture Signature and Windows Hotfixes Updates</b></li> <li><b>Automatically download Endpoint Profile Fingerprints</b></li> </ul>
<b>Firmware &amp; Patch Updates</b>	
<p><b>NOTE:</b> The Firmware &amp; Patch Updates table shows only the data that is known to Webservice or imported using the <b>Import Updates</b> button.</p> <p><b>NOTE:</b> Patch residual files under <code>/var/avenda/platform/backup</code>, <code>/var/avenda/platform/patches</code>, and <code>/var/avenda/platform/store/updates</code> seven days old and older are automatically deleted daily.</p>	
Import Updates	If the server is not able to reach the Webservice server, click <b>Import Updates</b> to import the latest signed Firmware and Update patch binaries (obtained via support or other means) into this server.

Parameter	Action/Description
	<p>These patch binaries will appear in the table and can be installed by clicking the <b>Install</b> button. When logged in as <i>appadmin</i>, you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands:</p> <ul style="list-style-type: none"> <li>• <b>system update</b> (for patches)</li> <li>• <b>system upgrade</b> (for upgrades)</li> </ul> <p>If a patch requires a prerequisite patch, that patch's <b>Install</b> button will not be enabled until the prerequisite patch is installed.</p>
Install	<p>The <b>Install</b> button appears after the update has been downloaded.</p> <p>Click <b>Install</b>.</p> <p>When you click <b>Install</b>, the installation of the update starts and the <b>Install Update</b> dialog box appears, showing the log messages that are generated.</p>
Re-Install	<p>Click <b>Re-Install</b> to reinstall a patch in the event the previous attempt to install fails.</p> <p>Reinstalling a patch is available only for the last installed patch.</p>
Uninstall	<p>To uninstall a skin, click <b>Uninstall</b> (for details, see <a href="#">Using the VMware vSphere Hypervisor Web Client to Install ClearPass on a Virtual Machine</a>).</p> <p><b>NOTE:</b> You cannot uninstall cumulative or point patch updates.</p>
Needs Restart	<p>The <b>Needs Restart</b> link appears when an update needs a reboot of the server in order to complete the installation.</p> <p>Clicking this link displays the <b>Install Update</b> dialog box, which shows the log messages generated during the installation.</p>
Installed	<p>The <b>Installed</b> link appears when an update has been successfully installed.</p> <p>Clicking this link displays the <b>Install Update</b> dialog box, which shows the log messages generated during the installation.</p>
Install Error	<p>This link appears when an update install encounters an error. Clicking this link displays the <b>Install Update</b> dialog box, which shows the log messages generated during the install.</p>
<b>Other</b>	
Check Status Now	<p>Click this button to perform an on-demand check for available updates. <b>Check Status Now</b> applies to updates only on a Publisher node, as well as Firmware &amp; Patch Updates.</p>
Delete	<p>Use this option to delete a downloaded update.</p>

## Changing the Administration Password

When the cluster password for this ClearPass server is set upon initial configuration (see [Completing the Virtual Appliance Setup on page 85](#)), the administration password is also set to the same password. If you wish to assign a unique **admin** password, use this procedure to change it.

To change the administration password:

1. In ClearPass, navigate to **Administration > Users and Privileges > Admin Users**.

The **Admin Users** page opens.

**Figure 60** Admin Users Page

The screenshot shows the 'Admin Users' page with the following details:

Administration » Users and Privileges » Admin Users

Admin Users

Add Import Export All Account Settings

Filter: User ID contains Go Clear Filter Show 10 records

#	User ID	Name	Privilege Level	Status
1.	admin	Super Admin	Super Administrator	Enabled
2.	apiadmin	API Admin	API Administrator	Enabled

Showing 1-2 of 2 Export Delete

2. Select the appropriate **admin** user.

The **Edit Admin User** dialog opens.

**Figure 61** Changing the Administration Password

The 'Edit Admin User' dialog box contains the following fields:

User ID:	admin
Name:	Super Admin
Password:	[REDACTED]
Verify Password:	[REDACTED]
Enable User:	<input checked="" type="checkbox"/> (Check to enable user)
Privilege Level	Super Administrator

Save Cancel

3. Change the administration password, verify the new password, then click **Save**.

## Powering Off the ClearPass Virtual Appliance

This procedure gracefully shuts down the virtual appliance without having to log in.

To power off the ClearPass virtual appliance:

1. Connect to the command-line interface by choosing **Action > Open Console**.
2. Enter the following commands:

- login: poweroff
- password: poweroff

The ClearPass virtual appliance shuts down.

# Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance

This section documents the procedures for installing the ClearPass Policy Manager virtual appliance on a host that runs Microsoft's hypervisor, Hyper-V™, as well as completing important administrative tasks, such as registering for ClearPass software updates and changing the admin password.

This section contains the following information:

- [Introduction](#)
- [Virtual Appliance Platforms](#)
- [Before Starting the ClearPass Installation](#)
- [ClearPass Hyper-V Virtual Appliance Installation Summary](#)
- [Importing the Virtual Machine](#)
- [Adding a Hard Disk to a Virtual Machine](#)
- [Launching the ClearPass Virtual Appliance](#)
- [Completing the Virtual Appliance Configuration](#)
- [Initial Login and Activation of the ClearPass Platform License](#)
- [Logging in to the ClearPass Virtual Appliance](#)
- [About Software Updates](#)
- [Software Updates Page](#)
- [Changing the Administration Password](#)
- [Powering Off the ClearPass Virtual Appliance](#)

## Introduction

Microsoft Hyper-V enables you to create and manage a virtualized computing environment by using virtualization technology that is built in to Windows Server. Installing Hyper-V installs the required components and optionally installs management tools.



---

This section assumes that Microsoft Hyper-V has been installed.

---

- For information about installing and starting Hyper-V on the Microsoft Windows Server 2012 R2 Enterprise with the Hyper-V Role, go to [Install Hyper-V Role](#).
- For information about installing and starting Hyper-V on Microsoft Windows Server 2012 R2, go to [Install Hyper-V](#).

## Supported Hypervisors

ClearPass supports the following hypervisors:

Hypervisor	Supported Versions
VMware vSphere Hypervisor (ESXi)	<ul style="list-style-type: none"><li>5.5</li><li>6.0</li><li>6.5 U1</li></ul>
Microsoft Hyper-V	<ul style="list-style-type: none"><li>Windows Server 2012 R2 with Hyper-V</li><li>Windows Server 2016 with Hyper-V</li><li>Windows Hyper-V Server 2012 R2</li><li>Windows Hyper-V Server 2016</li></ul>
 NOTE	For the latest information about supported hypervisors and virtual appliance system requirements, look in the appropriate version folders in the <b>Aruba Support Center &gt; Documentation &gt; Software User &amp; Reference Guides &gt; ClearPass &gt; Release Notes</b> .

## Meeting the Recommended Hyper-V Server Specifications

Please carefully review all virtual appliance requirements, including functional IOP ratings, and verify that your system meets these requirements. These recommendations supersede earlier requirements that were published for ClearPass Policy Manager 6.7 installations.

Virtual appliance recommendations are adjusted to align with the requirements for ClearPass hardware appliances. If you do not have the virtual appliance resources to support a full workload, you should consider ordering the ClearPass Policy Manager hardware appliance.

### Supplemental Storage/Hard Disk Requirements

ClearPassHyper-V ships with a 30 GB hard disk volume. This must be supplemented with additional storage/hard disk by adding a virtual hard disk (see [Adding a Hard Disk to a Virtual Machine on page 101](#) for details). The additional space required depends on the ClearPass virtual appliance version.

### Processing and Memory Requirements

To ensure scalability, dedicate or reserve the processing and memory to the ClearPass VM instance. You must also ensure that the disk subsystem can maintain the IOPs (I/O operations per second) throughput as detailed below.

#### ClearPass Server I/O Rate

Most virtualized environments use a shared disk subsystem, assuming that each application will have bursts of I/O without a sustained high I/O throughput. ClearPass Policy Manager requires a continuous sustained high data I/O rate.

## Virtual Appliance Platforms

Aruba provides three virtual appliance platforms, plus an evaluation platform:

- ClearPassPolicy Manager C1000V
- ClearPassPolicy Manager C2000V
- ClearPassPolicy Manager C3000V

- ClearPassPolicy Manager CLAV

## Before Starting the ClearPass Installation

Before starting the installation and configuration procedures for the virtual appliance, determine the following information for the ClearPass server on your network, note the corresponding values for the parameters listed in [Table 20](#), and keep it for your records:

**Table 20: ClearPass Server Configuration Information**

Required Information	Value for Your Installation
Host name (Policy Manager server)	
Management interface IP address	
Management interface subnet mask	
Management interface gateway	
Data interface IP address (optional)	<b>NOTE:</b> Make sure that the Data interface IP address is <i>not</i> in the same subnet as the Management interface IP address.
Data interface subnet mask (optional)	
Data interface gateway (optional)	
Primary DNS	
Secondary DNS	
NTP server (optional)	

## ClearPass Hyper-V Virtual Appliance Installation Summary

The process of installing the ClearPass Policy Manager virtual appliance on one or more hosts that runs Microsoft Hyper-V consists of four stages:

1. Download the Microsoft Hyper-V package from the **Download Software > ClearPass > Policy Manager > <Current Release Number> > Hyper-V** folder on the Aruba Support Center and unzip it to a folder on your server to extract the files.
2. Import the virtual machine.
  - a. Choose the import type.

- b. If required, specify the virtual switch that the Management Interface and Data Interface will be connected to.
3. Add a new virtual hard disk.
  - a. Configure the disk format, type, and size based on the requirements for your virtual appliance.
4. Power on and configure the virtual appliance.

Instructions for these procedures are provided in the following sections.

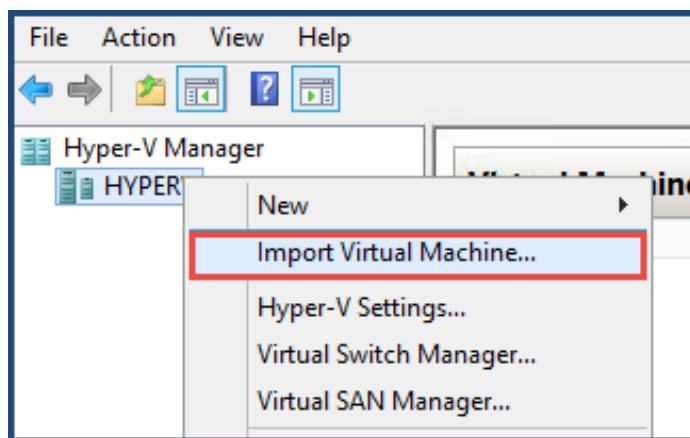
## Importing the Virtual Machine

Microsoft Hyper-V gives you the ability to import virtual appliances that have not been previously exported. This is extremely helpful in situations where a host OS becomes corrupted, or if the most recent good backup of a virtual appliance is a file-level backup of the host.

To import the virtual appliance:

1. Download the software image from the **Download Software > ClearPass > Policy Manager > <Current\_Release\_Number> > Hyper-V** folder on the Aruba Support Center and unzip it to a folder on your server to extract the files.
2. To extract the files, unzip the files to a folder on your server.
3. Open up the Hyper-V Manager Console.
4. From the Hyper-V Manager, select the **name of the Hyper-V server**, then right-click and select **Import Virtual Machine**.

**Figure 62** Selecting the "Import Virtual Machine" Option

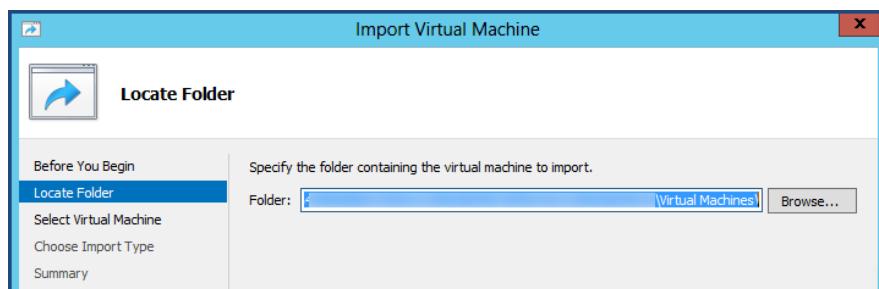


The **Before You Begin** dialog opens.

5. Click **Next**.

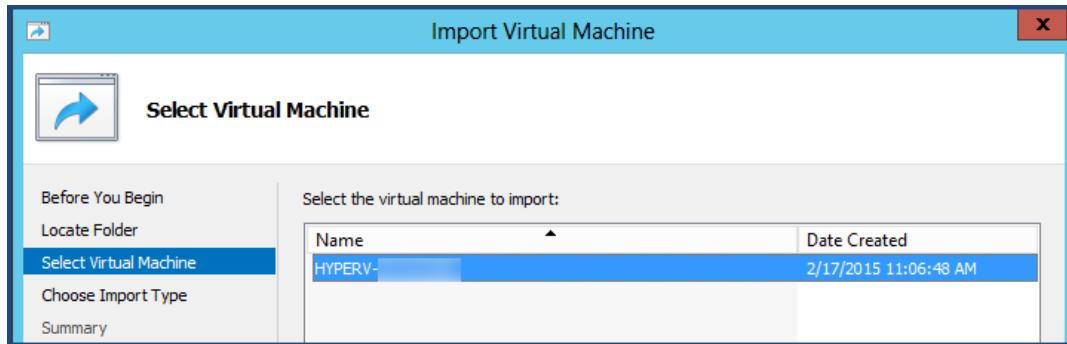
The **Locate Folder** dialog opens.

**Figure 63** Locating the Folder



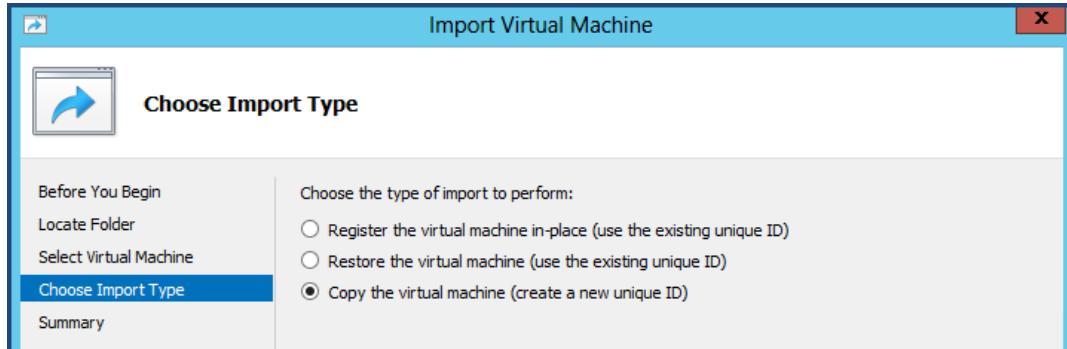
- In the **Locate Folder** step, select the folder you unzipped in **Step 2**, then click **Next**.  
The **Select Virtual Machine** dialog opens.

**Figure 64** Selecting the Virtual Machine



- Make sure the correct virtual appliance is highlighted, then click **Next**.  
The **Choose Import Type** dialog opens.

**Figure 65** Specifying the Import Type



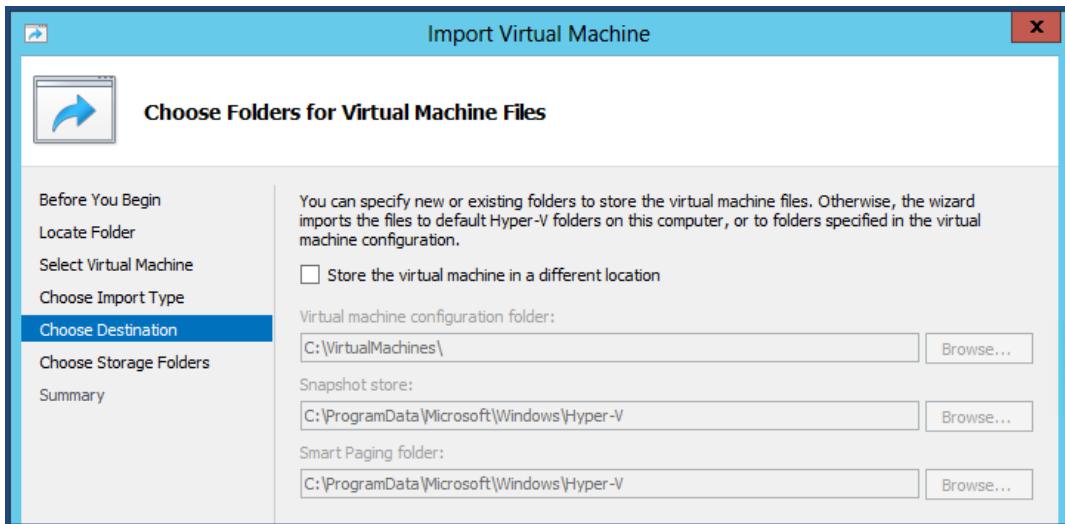
- In the **Choose Import Type** step, select **Copy the virtual machine**, then click **Next**.



When you choose **Copy the virtual machine**, Hyper-V creates new and unique identifiers for the virtual appliance.

The **Choose Folders for Virtual Machine Files** dialog opens.

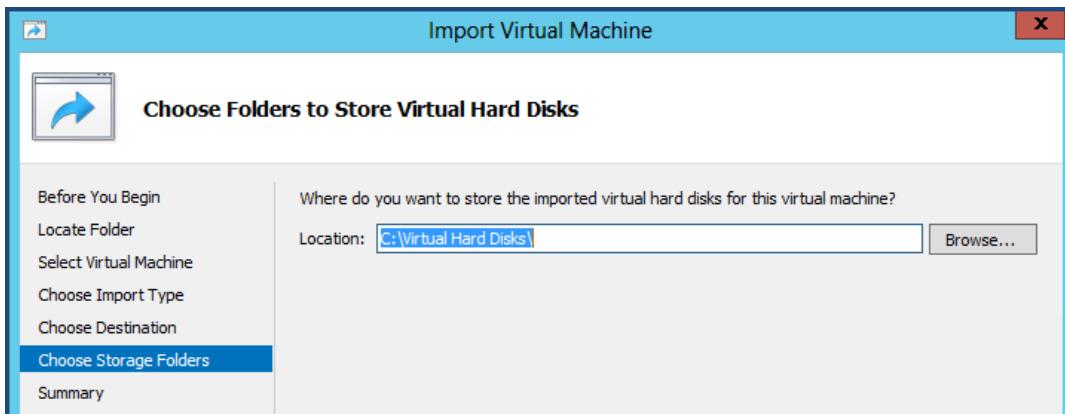
**Figure 66 Specifying the Folders for the Virtual Machine Files**



9. You can choose to either specify an alternate location to store the virtual appliance's files or accept the defaults:
  - a. To specify an alternate location to store the virtual appliance's files, click (enable) the **Store the virtual machine in a different location** check box, specify the following folders, then click **Next**:
    - Virtual machine configuration folder
    - Snapshot folder
    - Smart Paging folder
  - b. To accept the default folders for the virtual appliance's files, click **Next**.

The **Choose Folders to Store Virtual Hard Disks** dialog opens.

**Figure 67 Specifying Folders to Store Virtual Hard Disks**



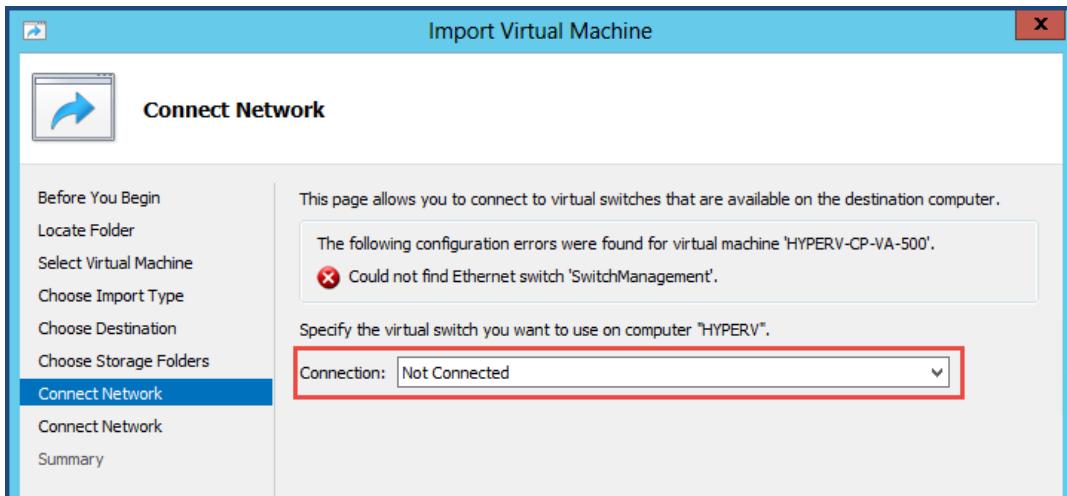
10. Accept the default virtual hard drive storage folder, or browse to a new location to change it to your preferred location, then click **Next**.

If the virtual appliance being imported was configured to use physical disks in pass-through mode, you will have the opportunity to either remove the storage from the virtual appliance's configuration or attach new physical disks in pass-through mode.

If an error occurs indicating that the virtual switch "SwitchManagement" could not be found, the **Connect Network** dialog opens.



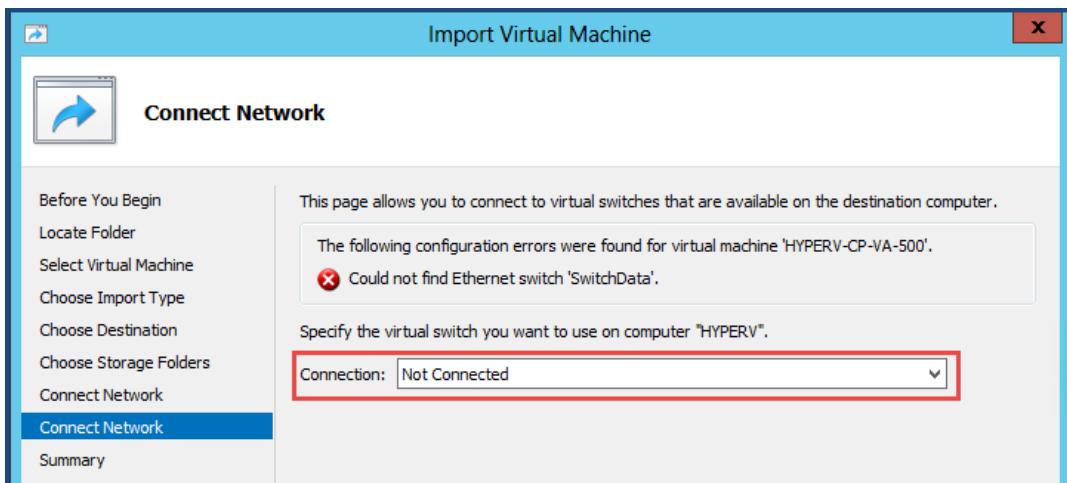
**Figure 68** Specifying the Virtual Switch in the Event of an Error



11. From the **Connection** drop-down, choose the virtual switch that will be used for the Management interface on the ClearPass Policy Manager virtual appliance, then click **Next**.

The following screen will be displayed to allow you to (optionally) specify the Data interface of the ClearPass Policy Manager virtual appliance.

**Figure 69** Specifying the Data Interface (Optional)



12. You can choose to either specify the virtual switch that will be used for the Data interface or bypass this dialog.
    - a. To specify the virtual switch that will be used for the Data interface, from the **Connection** drop-down, choose the virtual switch that will be used for the Data interface, then click **Next**.
    - b. To bypass this configuration option, leave **Not connected** selected in the **Connection** drop-down, then click **Next**.
- The **Completing Import Wizard** screen opens. This screen provides a summary of the import virtual appliance configuration that you specified.
13. Review the settings displayed in the **Summary** page, and if they are correct, click **Finish**.

This completes the procedure to import the virtual appliance.



## Adding a Hard Disk to a Virtual Machine

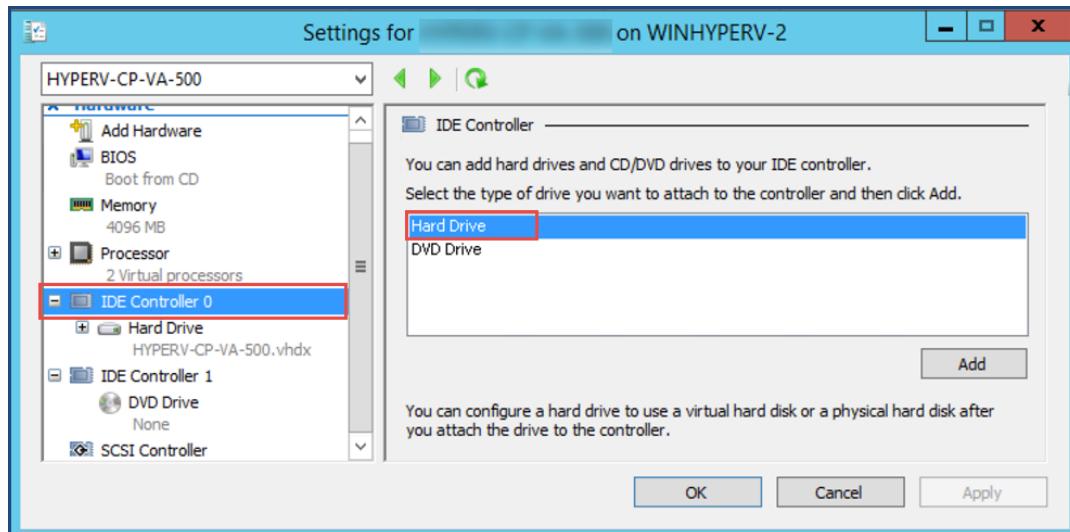
Do not create the virtual hard disk in a folder that is marked for encryption. Virtual hard disks are stored as .vhdx files. Hyper-V does not support the use of storage media if Encrypting File System (EFS) has been used to encrypt the .vhdx file. However, you can use files stored on a volume that uses Windows BitLocker Drive Encryption.

To add a hard disk to a virtual machine:

1. Open **Hyper-V Manager**.
2. In the **Results** pane, under **Virtual Machines**, select the virtual appliance that you want to configure.
3. In the **Action** pane, under the name of the virtual appliance, click **Settings**.

The **Settings** page opens.

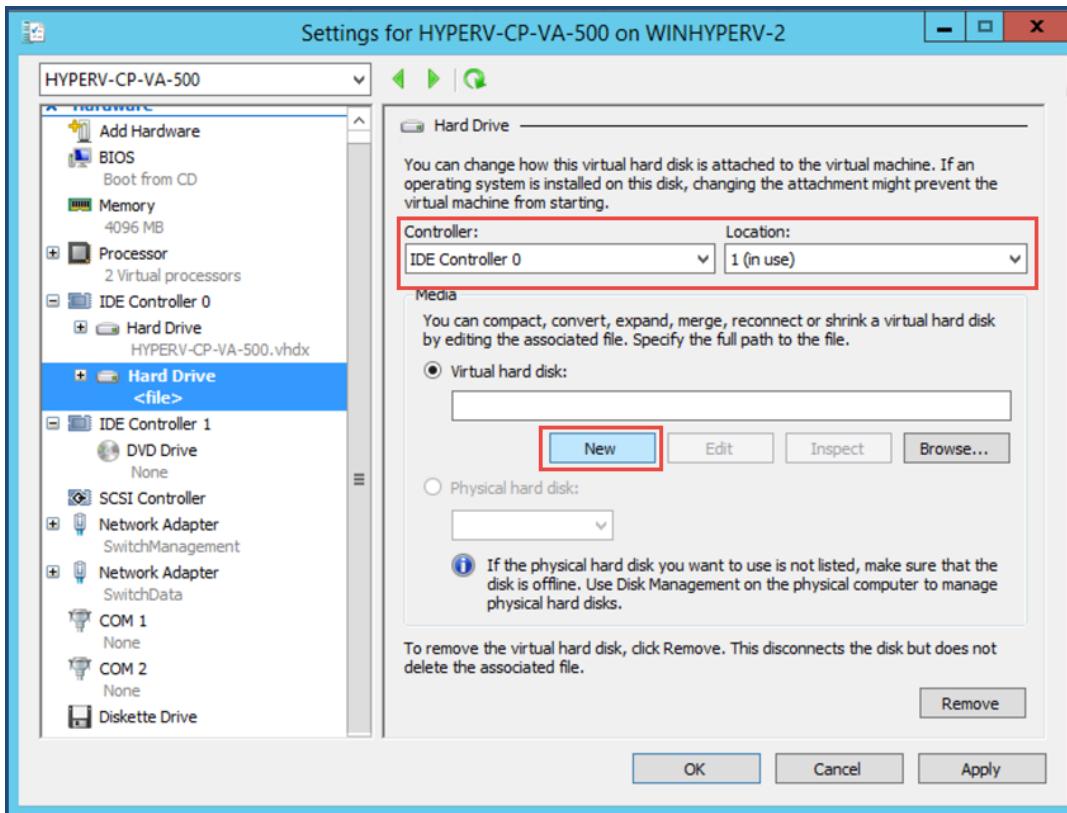
**Figure 70** Specifying the Controller



4. To select the controller to attach the virtual hard disk to, in the Navigation (left) pane, select **IDE Controller 0** (**Hard Drive** is selected by default), then click **Add**.

The **Hard Drive** dialog opens.

**Figure 71** Configuring the Hard Drive



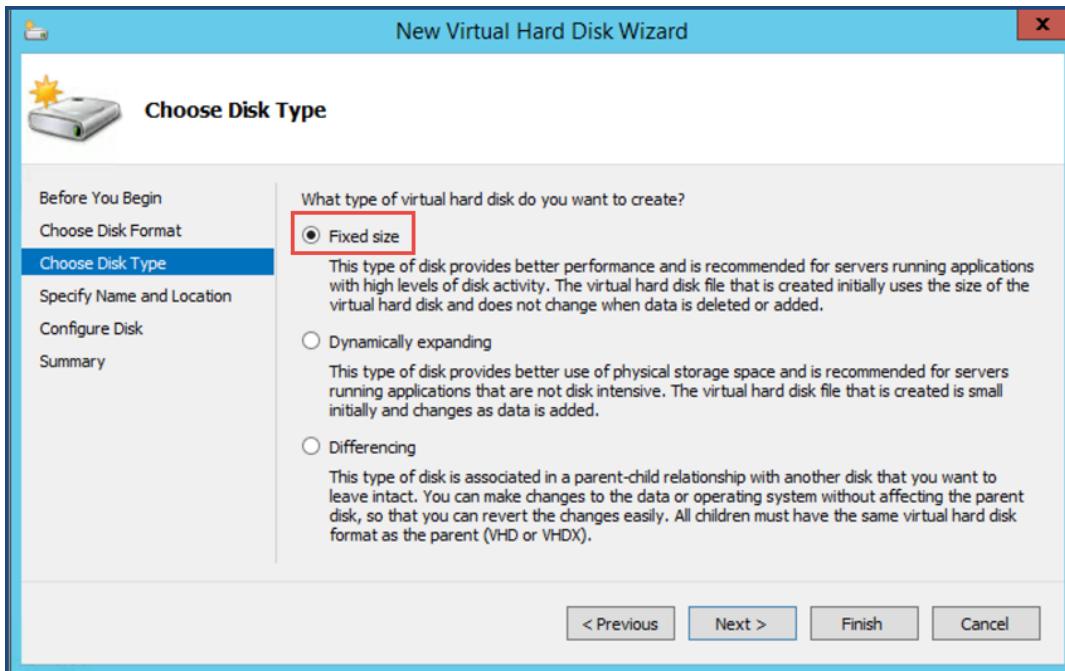
5. In the **Hard Drive** dialog:
  - a. **Controller:** Set to **IDE Controller 0**.
  - b. **Location:** Set to **1 (in use)**.
6. Below the **Virtual hard disk** field, click **New**.  
The **New Virtual Hard Disk Wizard** opens.
7. From the **Before You Begin** dialog, click **Next**.  
The **Choose Disk Format** dialog opens.

**Figure 72** Specifying the Disk Format



8. For the disk format, choose **VHDX**, then click **Next**.  
The **Choose Disk Type** dialog opens.

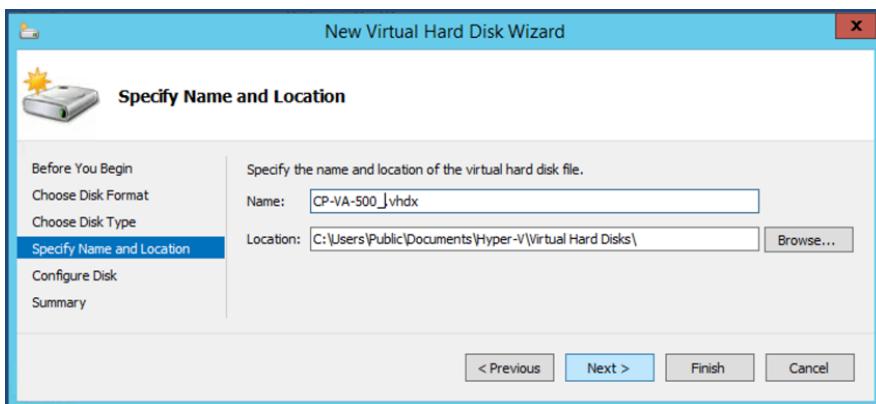
**Figure 73** Specifying the Virtual Hard Disk Type



9. For the disk type, choose **Fixed size**, then click **Next**.

The **Specify Name and Location** dialog opens.

**Figure 74** Specifying the Name and Location of the Hard Disk File

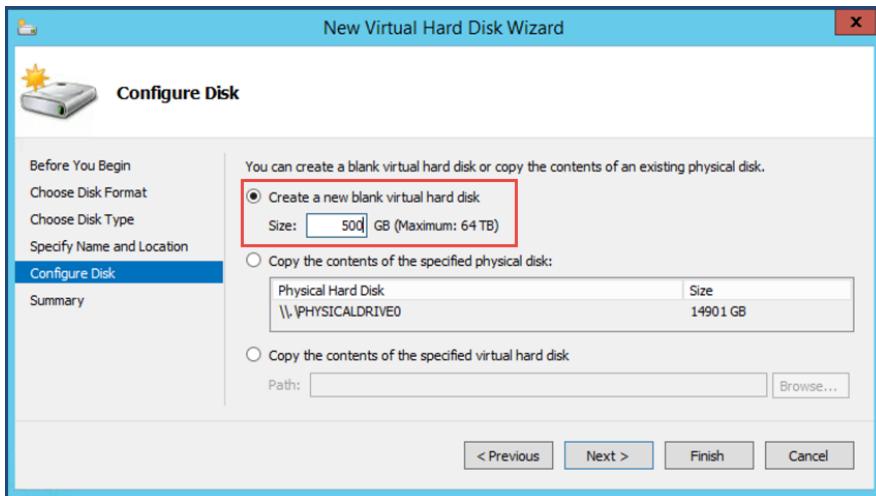


10. Do the following:

- a. Enter the name of the virtual hard disk file.
- b. Browse to the location of the virtual hard disk file, select it, then click **Next**.

The **Configure Disk** dialog opens.

**Figure 75** Configuring the New Virtual Hard Disk



11. Select **Create a new blank virtual hard disk**.

a. Then enter the size of the of virtual hard disk in Gigabytes (GB).

For the latest information on the recommended disk sizes for a virtual hard disk, refer to the Release Notes in the appropriate version folder in the **Aruba Support Center** at **Documentation > Software User & Reference Guides > ClearPass > Release Notes..**

b. Click **Next**.

The **Completing the New Virtual Hard Disk Wizard** screen opens.

12. Review the settings displayed in the **Summary** page, and if they are correct, click **Finish**.

This completes the procedure to add a virtual hard disk.

## Additional Virtual Hard Disk Considerations

Additional considerations to take into account when adding virtual hard disks are as follows:

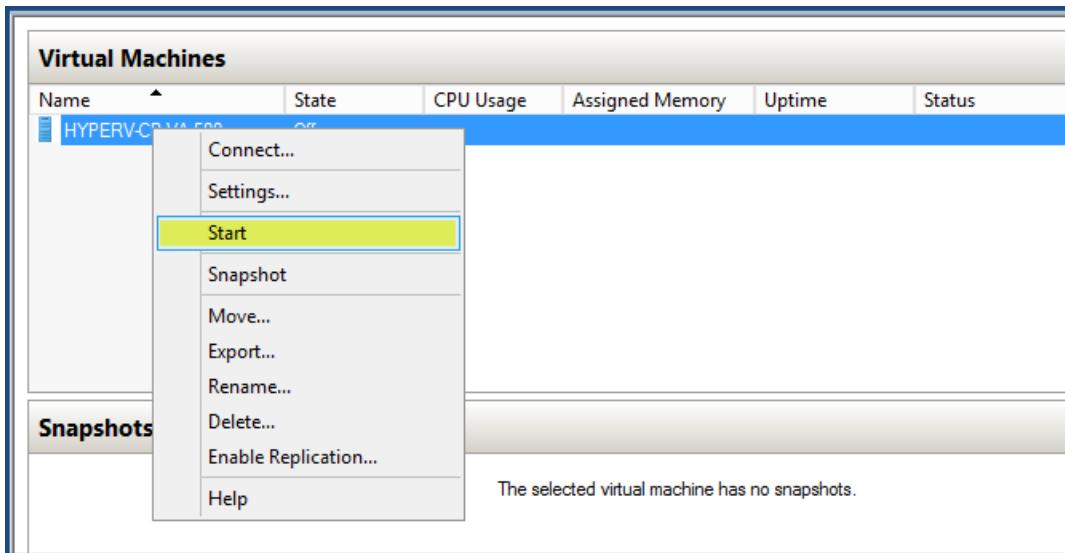
- By default, membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. However, an administrator can use Authorization Manager to modify the authorization policy so that a user or group of users can complete this procedure.
- Virtual hard disks are stored as .vhdx files, which makes them portable, but it also poses a potential security risk. We recommend that you mitigate this risk by taking precautions such as storing the .vhdx files in a secure location.
- The virtual hard disk is created when you click **Finish** to complete the wizard. Depending on the options you choose for the virtual hard disk, the process can take a considerable amount of time.
- Virtual hard disks cannot be stored in a folder that uses New Technology File System (NTFS) compression.
- You can make certain changes to a virtual hard disk after you create it. For example, you can convert it from one type of virtual hard disk to another. You can use the **Edit Virtual Hard Disk** wizard to make these changes.

## Launching the ClearPass Virtual Appliance

To launch the ClearPass virtual appliance:

1. To power on the virtual appliance, from the ClearPass Policy Manager appliance, right-click the **name of the virtual machine**, then choose **Start**.

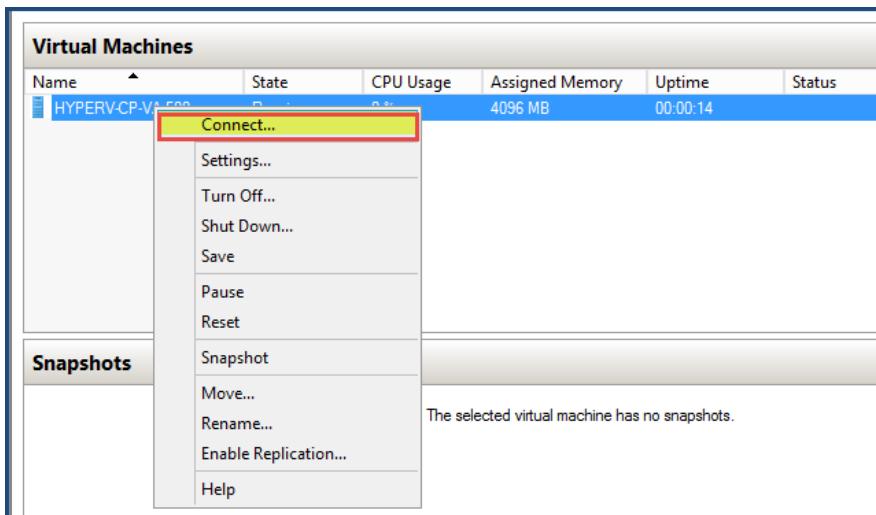
**Figure 76 Starting the Virtual Machine**



The virtual appliance powers on.

2. To launch the VM console, right-click the **name of the virtual machine**, then choose **Connect**.

**Figure 77 Launching the VM Console**



The initial virtual machine console screen is displayed. At the bottom of the console screen is the following prompt:

*Enter 'y' or 'Y' to proceed:*

3. To proceed with the installation, enter **y**.

ClearPass setup and installation begins.

The console screen appears.

4. Enter the **number** for the appropriate appliance type (do not enter the appliance model itself).

For example, to specify the **C3000V** appliance, you would enter the number **4**. Options include:

- **1) CLABV**
- **2) C1000V**
- **3) C2000V**
- **4) C3000V**

The system requirements are displayed for the appliance model you entered, along with your current system configuration.

5. Compare these to make sure your system meets the new system requirements.
6. When you have verified that your system meets the new requirements, press **y**. ClearPass will reboot at least once.

Two console screens appear sequentially—the first screen indicates that the ClearPass Installer is rebooting, and the second screen indicates that the virtual appliance is rebooting.

When the rebooting process is complete, the ClearPass virtual appliance is configured, and the virtual appliance will power on and boot up within a couple of minutes. The whole process typically takes between 30 and 40 minutes.

7. After the ClearPass virtual appliance launches correctly, the virtual appliance login banner is displayed.
8. Proceed to the next section, [Completing the Virtual Appliance Configuration](#).

## Completing the Virtual Appliance Configuration

To complete the virtual appliance configuration:

1. Refer to and note the required ClearPass server configuration information listed in [Table 20](#).
2. **Log in to the virtual appliance** using the following preconfigured credentials :
  - login: **appadmin**
  - password: **<password>**

This initiates the Policy Manager Configuration wizard.

3. **Configure the ClearPass virtual appliance.**

Follow the prompts, replacing the placeholder entries in the following illustration with the information you entered in [Table 20](#).

- Enter hostname:
- Enter Management Port IP Address:
- Enter Management Port Subnet Mask:
- Enter Management Port Gateway:
- Enter Data Port IP Address:
- Enter Data Port Subnet Mask:
- Enter Data Port Gateway:
- Enter Primary DNS:
- Enter Secondary DNS:

4. **Specify the cluster password.**

 Setting the cluster password also changes the password for the CLI user **appadmin**, as well as the Administration user **admin**. If you want the **admin** password to be unique, see [Changing the Administration Password on page 113](#).

- a. Enter any string with a minimum of six characters, then you are prompted to confirm the cluster password.
  - b. After this configuration is applied, use this new password for cluster administration and management of the ClearPass virtual appliance.
5. **Configure the system date and time.**
    - a. Follow the prompts to configure the system date and time.
    - b. To set the date and time by configuring the NTP server, use the primary and secondary NTP server information you entered in [Table 20](#).

## 6. Apply the configuration.

- a. To apply the configuration, press **Y**.
  - To restart the configuration procedure, press **N**.
  - To quit the setup process, press **Q**.

Configuration on the virtual appliance console is now complete. The next task is to activate the ClearPass Platform license.

## Initial Login and Activation of the ClearPass Platform License

Upon initial login to a ClearPass 6.7 server, you are prompted to enter the ClearPass Platform License Key. The ClearPass 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.

To specify the ClearPass Platform license upon initial login:

1. After the configuration has been applied at the virtual appliance console, open a web browser and go to the management interface of ClearPass Policy Manager: <https://x.x.x.x/tips/>, where **x.x.x.x** is the IP address of the management interface defined for the ClearPass server in [Table 20](#).
2. Log in to the ClearPass 6.7 server.
3. Accept any security warnings from your browser regarding the self-signed SSL certificate, which comes installed in ClearPass by default.

The ClearPass Policy Manager End-User Software License Agreement dialog is displayed.

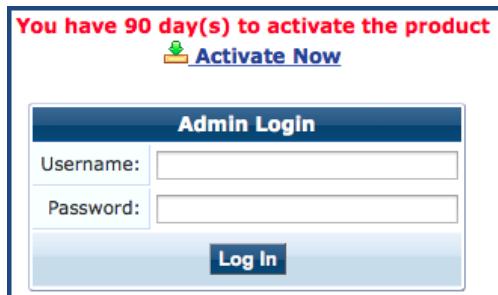
**Figure 78** Entering the ClearPass Platform License Key



4. Enter the ClearPass Platform License Key.
5. Click the check box for **I agree to the above terms and conditions**.  
The **Add License** button is now enabled.
6. Click **Add License**.

Upon successfully entering the Platform License Key, 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 79** Activating ClearPass



7. To activate ClearPass on this virtual appliance, click **Activate Now**.

ClearPass Policy Manager attempts to activate the license over the Internet with Aruba license activation servers.

If the ClearPass Policy Manager virtual appliance does not have Internet access, you can perform the license activation offline by following the steps for offline activation presented in the **Offline Activation** section shown in [Figure 80](#).

**Figure 80** Activating the ClearPass Platform License



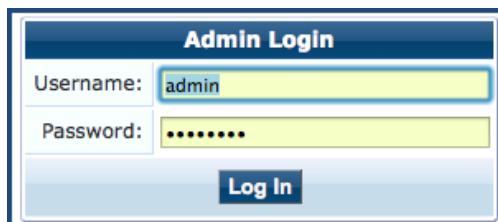
8. If the ClearPass server is connected to the Internet, click the **Activate Now** button.

After successfully activating ClearPass online, you will see a message above the **Admin Login** screen indicating that the product has been successfully activated.

## Logging in to the ClearPass Virtual Appliance

After a successful Platform License activation, the **Admin Login** dialog opens.

**Figure 81** Logging in to the ClearPass Virtual Appliance



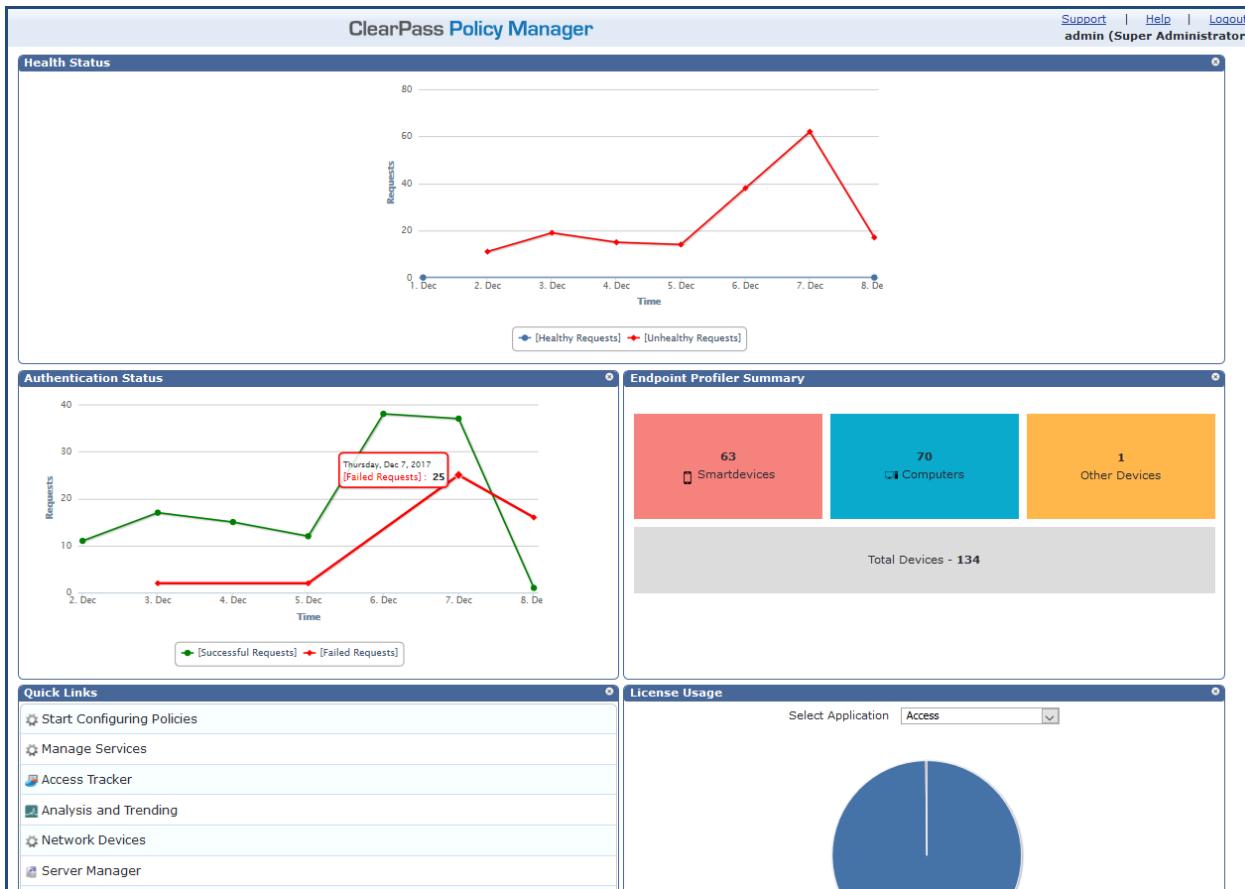
9. Log in to the ClearPass virtual appliance with the following credentials:

- **Username:** admin
- **Password:** Enter the cluster password defined in [Completing the Virtual Appliance Configuration on page 106](#).

10. Click **Log In**.

The ClearPass Policy Manager Landing Page opens.

**Figure 82** ClearPass Policy Manager Landing Page



## About Software Updates

This section describes the ClearPass server software update process.

ClearPass 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 configure 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 83](#) displays the **Software Updates** page:

**Figure 83** Software Updates Page

The screenshot shows the 'Software Updates' page with the following sections:

- HPE Passport Credentials:** Fields for Username (HPEpassport@hpe.com) and Password (redacted), with a **Save** button.
- Posture & Profile Data Updates:** A table showing three entries:

Update Type	Data Version	Data Created	Last Update	Last Updated	Update Status
Posture Signature Updates*	1.49236	2017/11/01 13:30:05	Online	2017/11/01 22:00:03	Updated 1 day ago
Windows Hotfixes Updates*	1.2181	2017/10/31 16:50:27	Online	2017/11/01 22:00:05	Updated 1 day ago
Endpoint Profile Fingerprints*	2.545	2017/10/24 11:15:29	File	2017/11/01 15:06:21	Updated 1 day ago

**Import Updates** button.

\* Automatic download and install is disabled  
To manually import Posture & Profile Data Updates, refer to Help for this page.
- Firmware & Patch Updates:** A table showing three entries:

Update Type	Name	Version	Size (MB)	Update Released	Last Checked	Status	Delete
Patch	6.7.0.100772*	-	0.0040	2017/11/15	2017/11/02 16:10:22	<b>Download</b>	-
Patch	ClearPass OnGuard Engine 1.0 Update 1 <sup>+</sup>	1.0.0.101255	62.7049	2017/10/30	2017/11/02 16:10:22	<b>Installed</b>	-
Guest Skin	Fidelity Investments Skin	0.1.6-0	0.6084	2013/09/09	2017/11/02 16:10:22	<b>Download</b>	-

**Import Updates** button.

\* Needs Restart  
+ Restarts Administration UI  
! Last Installed, available for Re-Install

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

**Table 21: Software Updates Page Parameters**

Parameter	Action/Description
<b>HPE Passport Credentials</b>	
HPE Passport Credentials	<p>Enter the <b>HPE Passport Credentials</b> provided to you.</p> <p>This text box is enabled only on a Publisher node.</p> <p>The first time the HPE Passport Credentials are saved, the ClearPass server performs the following operations:</p> <ul style="list-style-type: none"> <li>Contacts the Webservice server to download the latest Posture &amp; Profile Data updates (depending on the Cluster-Wide Parameter settings for those parameters).</li> <li>Checks for any available firmware and patch updates.</li> </ul>
<b>Posture &amp; Profile Data Updates</b>	
Import Updates	<p>To download the Posture and Profile Data Updates to the client (for example, a Windows laptop):</p> <ol style="list-style-type: none"> <li>From the client device, log in to the <a href="#">Aruba Support Center</a>.</li> <li>Select the <b>Download Software</b> tab, then navigate to <b>ClearPass &gt; Tools &gt; Posture &amp; Profile Data Updates</b>.</li> <li>Click the desired update(s) (which are in zip file format) and save the file.</li> <li>From ClearPass, click the <b>Posture and Profile Data Updates &gt; Import Updates</b> button to import the downloaded file into ClearPass.</li> </ol> <p><b>NOTE:</b> In a ClearPass cluster, the <b>Import Updates</b> option is available on the Publisher node only.</p> <p>By default, updates for <b>Posture Signature</b>, <b>Windows Hotfixes</b>, and <b>Endpoint Profile Fingerprints</b> are <i>not</i> automatically downloaded and installed. To set these updates to be automatic, you must set the following <i>Cluster-Wide Parameters</i> to <b>TRUE</b>:</p> <ul style="list-style-type: none"> <li><b>Automatically download Posture Signature and Windows Hotfixes Updates</b></li> <li><b>Automatically download Endpoint Profile Fingerprints</b></li> </ul>
<b>Firmware &amp; Patch Updates</b>	
<p><b>NOTE:</b> The Firmware &amp; Patch Updates table shows only the data that is known to Webservice or imported using the <b>Import Updates</b> button.</p> <p><b>NOTE:</b> Patch residual files under <code>/var/avenda/platform/backup</code>, <code>/var/avenda/platform/patches</code>, and <code>/var/avenda/platform/store/updates</code> seven days old and older are automatically deleted daily.</p>	
Import Updates	If the server is not able to reach the Webservice server, click <b>Import Updates</b> to import the latest signed Firmware and Update patch binaries (obtained via support or other means) into this server.

Parameter	Action/Description
	<p>These patch binaries will appear in the table and can be installed by clicking the <b>Install</b> button. When logged in as <i>appadmin</i>, you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands:</p> <ul style="list-style-type: none"> <li>● <b>system update</b> (for patches)</li> <li>● <b>system upgrade</b> (for upgrades)</li> </ul> <p>If a patch requires a prerequisite patch, that patch's <b>Install</b> button will not be enabled until the prerequisite patch is installed.</p>
Install	<p>The <b>Install</b> button appears after the update has been downloaded.</p> <p>Click <b>Install</b>.</p> <p>When you click <b>Install</b>, the installation of the update starts and the <b>Install Update</b> dialog box appears, showing the log messages that are generated.</p>
Re-Install	<p>Click <b>Re-Install</b> to reinstall a patch in the event the previous attempt to install fails.</p> <p>Reinstalling a patch is available only for the last installed patch.</p>
Uninstall	<p>To uninstall a skin, click <b>Uninstall</b> (for details, see <a href="#">Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance</a>).</p> <p><b>NOTE:</b> You cannot uninstall cumulative or point patch updates.</p>
Needs Restart	<p>The <b>Needs Restart</b> link appears when an update needs a reboot of the server in order to complete the installation.</p> <p>Clicking this link displays the <b>Install Update</b> dialog box, which shows the log messages generated during the installation.</p>
Installed	<p>The <b>Installed</b> link appears when an update has been successfully installed.</p> <p>Clicking this link displays the <b>Install Update</b> dialog box, which shows the log messages generated during the installation.</p>
Install Error	<p>This link appears when an update install encounters an error. Clicking this link displays the <b>Install Update</b> dialog box, which shows the log messages generated during the install.</p>
Other	
Check Status Now	<p>Click this button to perform an on-demand check for available updates. <b>Check Status Now</b> applies to updates only on a Publisher node, as well as Firmware &amp; Patch Updates.</p>
Delete	<p>Use this option to delete a downloaded update.</p>

## Changing the Administration Password

When the cluster password for this ClearPass server is set upon initial configuration (see [Completing the Virtual Appliance Configuration on page 106](#)), the administration password is also set to the same password. If you wish to assign a unique **admin** password, use this procedure to change it.

To change the administration password:

1. In ClearPass, navigate to **Administration > Users and Privileges > Admin Users**.

The **Admin Users** page opens.

**Figure 84** Admin Users Page

The screenshot shows the 'Admin Users' page with the following details:

#	User ID	Name	Privilege Level	Status
1.	admin	Super Admin	Super Administrator	Enabled
2.	apiadmin	API Admin	API Administrator	Enabled

Filter: User ID contains [ ] Go Clear Filter Show 10 records Export Export All Account Settings

Showing 1-2 of 2 Export Delete

2. Select the appropriate **admin** user.

The **Edit Admin User** dialog opens.

**Figure 85** Changing the Administration Password

The 'Edit Admin User' dialog has the following fields:

User ID:	admin
Name:	Super Admin
Password:	[REDACTED]
Verify Password:	[REDACTED]
Enable User:	<input checked="" type="checkbox"/> (Check to enable user)
Privilege Level	Super Administrator

Save Cancel

3. Change the administration password, verify the new password, then click **Save**.

## Powering Off the ClearPass Virtual Appliance

This procedure gracefully shuts down the virtual appliance without having to log in.

To power off the ClearPass virtual appliance:

1. To connect to the command-line interface, right-click the **name of the virtual machine**, then choose **Connect**.
2. Enter the following commands:
  - login: poweroff
  - password: poweroff

The ClearPass virtual appliance shuts down.

This chapter includes the following information:

- [ClearPass Cluster Overview](#)
- [Cluster Design Considerations](#)
- [About Large Scale Deployments](#)
- [Deploying the Standby Publisher](#)
- [Adding a Subscriber Node to the Publisher](#)
- [Rejoining a Down Node to the Cluster](#)
- [Deploying ClearPass Insight in a Cluster](#)
- [Configuring Cluster File-Backup Servers](#)
- [Cluster CLI Commands](#)

## ClearPass Cluster Overview

This section contains the following information:

- [Introduction](#)
- [ClearPass Databases](#)
- [Publisher/Subscriber Model](#)
- [Network Ports That Must Be Enabled](#)
- [Cluster Scaling Limitations](#)

### Introduction

A *cluster* is a logical connection of any combination of ClearPass hardware or virtual appliances.

This chapter provides guidance on how to design and deploy ClearPass Policy Manager clusters, how to complete major tasks such as adding a Subscriber node and deploying a standby Publisher, as well as how to rejoin a down node to the cluster. Finally, the set of cluster-specific CLI commands is included.

ClearPass hardware appliance models are:

- **C1000:** Provides advanced policy control for up to 500 simultaneous sessions.
- **C2000:** Provides advanced policy control for up to 5,000 simultaneous sessions.
- **C3000:** Provides advanced policy control for up to 25,000 simultaneous sessions.

The ClearPass virtual appliances are distributed as a single image, which becomes a **CLABV** (provided for testing purposes), **C1000V**, **C2000V**, or **C3000V**, depending on the amount of virtual hardware that is allocated.

ClearPass Policy Manager can be deployed either as a dedicated hardware appliance or a virtual machine running on top of VMware vSphere Hypervisor or Microsoft Hyper-V. For more information on the Aruba hardware and virtual appliances, refer to [Setting Up the ClearPass Hardware and Virtual Appliances on page 60](#).

When demand exceeds the capacity of a single instance, or you have a requirement for a High Availability deployment, you have the option of logically joining multiple instances to process the workload from the network.

You can logically join physical and virtual instances and also join ClearPass instances that are dissimilar in size. However, careful planning must be taken, especially if you plan to utilize the failover capabilities within the clustering feature.

The cluster feature allows for shared configuration and databases. However, it does not provide a virtual IP address for the cluster, so failover/redundancy for captive portal for Guest relies on Domain Name System (DNS) lookup or load balancing.

RADIUS clients must define a primary and backup RADIUS server.

## Authentication Requests in a Cluster

The typical use case for Policy Manager is to process authentication requests using the policy framework. The policy framework is a selection of services that work to process authentication requests, but the policy framework also determines authentication, authorization, posture, enforcement, role, etc. of the endpoint/end-user.

In the context of cluster operations, authentication typically involves a read-only operation from the configuration database. A cluster node receives an authentication request, determines the appropriate policies to apply, and responds appropriately. This does not require a configuration change, and can therefore be scaled across the entire cluster.



Authentication is performed from the node itself to the configured identity store, whether locally (as synchronized by the Publisher; for example, a Guest account) or externally, such as with Microsoft Active Directory.

Logs relevant to each authentication request are recorded separately on each node, using that node's log database. Centralized reporting is handled by generating a Netevent from the node, which is sent to all Insight nodes and recorded in the Insight database (for related information, see [Deploying ClearPass Insight in a Cluster on page 136](#)).

## ClearPass Databases

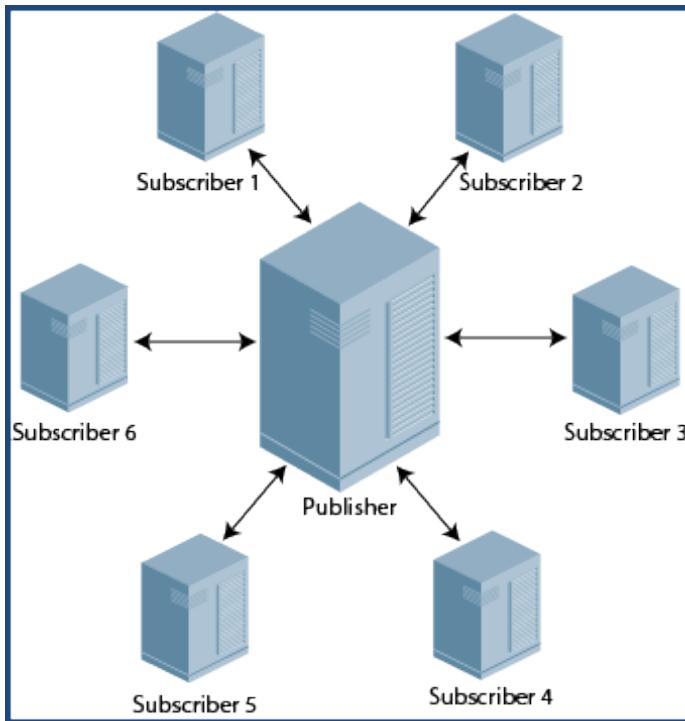
Each ClearPass server makes use of the following databases:

- **Configuration database.** Contains most of the editable entries that can be seen in the ClearPass user interface. This includes, but is not limited to:
  - Administrative user accounts
  - Local user accounts
  - Service definitions
  - Role definitions
  - Enforcement policies and profiles
  - Network access devices
  - Guest accounts
  - Onboard certificates
  - Most of the configuration shown within Guest and Onboard
- **Log database.** Contains activity logs generated by typical usage of the system. This includes information shown in Access Tracker and the Event Viewer.
- **Insight database.** Records historical information generated by the Netevents framework. This database is used to generate reports (for related information, see [Deploying ClearPass Insight in a Cluster on page 136](#)).

## Publisher/Subscriber Model

ClearPass uses a Publisher/Subscriber model to provide multiple-box clustering. Another term for this model is *hub and spoke*, where the hub corresponds to the Publisher, and the spokes correspond to the Subscribers.

**Figure 86** Publisher and Subscribers in Hub and Spoke Configuration



- The **Publisher node** functions as the master controller in a cluster. The Publisher is your central point of configuration, monitoring, and reporting. It is also the central point of database replication. All the databases are managed through the Publisher.
  - There is at most one active Publisher in this model, and a potentially unlimited number of Subscribers.
  - The Publisher node has full read/write access to the configuration database. All configuration changes must be made on the Publisher. The Publisher node sends configuration changes to each Subscriber node.
- The **Subscriber nodes** are worker nodes. All the AAA load, all RADIUS requests, and the node where policy decisions are being made are on the Subscriber nodes.
  - Subscriber nodes maintain a local copy of the configuration database, and each Subscriber has read-only access to a local copy of the configuration database.

Network Address Translation (NAT) is not supported between the Publisher and Subscriber nodes.

### What Information Is Replicated?

A background replication process handles the task of updating the configuration database based on the configuration changes received from the Publisher.

Multiple entities exist within a ClearPass server cluster that must be shared to ensure successful operation of the cluster. Only the configuration database is replicated.

The Log and Insight databases are not replicated across the cluster.



However, certain elements are node-specific and these must be configured separately for each node, which you can achieve directly on the Publisher or individually on the Subscriber node.

### Elements Replicated

Cluster replication is delta-based; that is, only changed information is replicated.

The cluster elements that are replicated across all the nodes in the cluster are as follows:

- All policy configuration elements
- All audit data
- All identity store data
  - Guest accounts, endpoints, and profile data
- Runtime information
  - Authorization status, posture status, and roles
  - Connectivity information, NAS details
- Database replication on port 5432 over SSL
- Runtime replication on port 443 over SSL

### Elements Not Replicated

The following elements are not replicated:

- Access Tracker logs and Session logs
- Authentication records
- Accounting records
- System events (Event Viewer data)
- System monitoring data

### Network Ports That Must Be Enabled

[Table 22](#) lists the network ports that must be opened between the Publisher and the Subscriber nodes.

**Table 22: Network Ports to Be Enabled**

Port	Protocol	Description
80	HTTP	Internal proxy
123	UDP	TNTP: Time synchronization
443	TCP	HTTPS: Internal proxy and node-to-node service
5432	TCP	PostgreSQL: Database replication

Because any Subscriber node can be promoted to be the Publisher node, all port/protocol combinations listed in [Table 22](#) should be:

- Bidirectional
- Open between any two nodes in the cluster

## Cluster Scaling Limitations

Due to the design requirements of the cluster Publisher/Subscriber model, various ClearPass components scale differently (see [Table 23](#)).

**Table 23:** *ClearPass Cluster Scaling Limitations*

Component	Scaling Limitation
Authentication capacity	Scales linearly according to the number of Subscriber nodes. Add more nodes as necessary to provide additional capacity to service authentication requests.
Configuration changes (Guest/ Onboard)	These configuration changes do not scale with additional nodes as they are centralized. Requires the Publisher be scaled to support write traffic from the maximum number of Subscribers that would be active concurrently.
Configuration changes (Policy Manager)	As the total size of the configuration set is bounded, these configuration changes are assumed to be infrequent and therefore not a significant limit to scaling.
Insight reports	Because this function is centralized, reporting does not scale with additional nodes. Use a separate Insight node sufficient to handle the incoming Netevents traffic from all nodes in the cluster. In a very large-scale deployment, the Publisher node should not be used as the Insight reporting node.
Logging capacity	Scales linearly according to the number of Subscriber nodes, as each node handles its own logging operations.
Replication load on Publisher	Scales linearly according to the number of Subscriber nodes. The replication is efficient as only changed information is sent.

## Cluster Design Considerations

This section contains the following information:

- [Cluster Deployment Sizing Guidance](#)
- [Publisher Node Guidelines](#)
- [Subscriber Node Guidelines](#)
- [Providing Sufficient Bandwidth Between Publisher and Subscribers](#)
- [Round-Trip Time Considerations for Geographically Distributed Clusters](#)
- [Implementing ClearPass Zones for Geographical Regions](#)

This section contains recommendations on how to optimize the Publisher and Subscriber constraints when deploying a ClearPass cluster.

## Cluster Deployment Sizing Guidance

Cluster deployment sizing should not be based on raw performance numbers.



---

When designing large clusters, we recommend contacting your Aruba account team to discuss options.

---

To determine the optimum sizing for a ClearPass cluster:

1. Determine how many endpoints need to be authenticated.
  - a. The number of authenticating endpoints can be determined by taking the number of users times the number of devices per user.
  - b. To this total, add the other endpoints that just perform MAC authentication, such as printers and other non-authenticating endpoints.
2. Take into account the following factors:
  - a. Number and type of authentications and authorizations:
    - MAC authentication/authorizations vs. PAP vs. EAP-MSCHAPv2 vs. PEAP-MSCHAPv2 vs. PEAP-GTC vs. EAP-TLS
    - Active Directory vs. local database vs. external SQL datastore
    - No posture assessment vs. in-band posture assessment in the PEAP tunnel vs. HTTPS-based posture assessment done by OnGuard.
  - b. RADIUS accounting load.
  - c. Operational tasks taking place during authentications, such as configuration activities, administrative tasks, replication load, periodic report generation, and so on.
  - d. Disk space consumed.

Note that ClearPass Policy Manager writes copious amounts of data for each transaction (this data is displayed in the Access Tracker).

3. Then pick the number of ClearPass hardware appliances you would need, with redundancy ranging from (N+1) to full redundancy, depending on the needs of the customer.

## Publisher Node Guidelines

### Setting Up a Standby Publisher

ClearPass Policy Manager allows you to designate one of the Subscriber nodes in a cluster to be the *Standby Publisher*, thereby providing for that Subscriber node to be automatically promoted to active Publisher status in the event that the Publisher goes out of service. This ensures that any service degradation is limited to an absolute minimum. For details, see [Deploying the Standby Publisher on page 127](#).

### Publisher Node Sizing

The Publisher node must be sized appropriately because it handles database write operations from all Subscribers simultaneously.

The Publisher must also be capable of handling the total-number of endpoints within the cluster and be capable of processing remote work directed to it when guest-account creation and onboarding are occurring.

### Publisher Deployment Guidance

- In a world-wide large-scale deployment, not all Subscriber nodes are equally busy. To determine the maximum request rate that must be handled by the Publisher node, examine the cluster's traffic pattern for busy hours and estimate the traffic load for each Subscriber node, adjusting for time zone differences.
- In a large-scale deployment, isolate the Publisher node, to allow it to handle the maximum amount of traffic possible.

- To help reduce the maximum amount of traffic possible in a large-scale deployment (ignoring API requests from Subscribers as well as the outbound replication traffic to Subscribers), the Publisher should not receive any authentication requests or Guest/Onboard requests directly .
- If the worker traffic sent from the Subscriber nodes is expected to fully saturate the capacity of the Publisher node, Insight should not be enabled on the Publisher node. If the Publisher node has spare capacity, it can be used to support the ClearPass Insight database. However, take care to carefully monitor the Publisher node's capacity and performance.

## **Subscriber Node Guidelines**

Guidelines for Subscriber node deployment are as follows:

### **Using Nearest Subscriber Node**

Guests and Onboard clients should be directed to the nearest Subscriber node. From the client's point of view, the internal API call to the Publisher is handled transparently. The best response time for static resources is obtained if the server is nearby.

### **Using Subscriber Nodes as Workers**

Subscriber nodes should be used as workers that process the following:

- Authentication requests (for example, RADIUS, TACACS+, Web-Auth)
- Online Certificate Status Protocol (OCSP) requests
- Static content delivery (for example, images, CSS, JavaScript)

### **Avoid Sending Worker Traffic to the Publisher**

Avoid sending "worker traffic" to the Publisher, as the Publisher services API requests from Subscribers, handles the resulting database writes, and generates replication changes to send back to the Subscribers.

### **If Onboard is Being Used**

If Onboard is used, ensure that the EAP-TLS authentication method in Policy Manager is configured to perform *localhost* OCSP (Online Certificate Status Protocol) checks.

## **Providing Sufficient Bandwidth Between Publisher and Subscribers**

In a large-scale deployment, reduced bandwidth or high latency on the link (greater than 200 ms) delivers a lower-quality user experience for all users of that Subscriber, even though static content is delivered locally almost instantaneously.

For reliable operation of each Subscriber, ensure that there is sufficient bandwidth available for communications with the Publisher. For basic authentication operations, there is no specific requirement for high bandwidth. However, the number of round-trips to complete an EAP authentication could cause delay for the end user.

### **Traffic Flows Between Publisher and Subscriber**

The traffic flows between the Publisher and Subscriber nodes include:

- Basic monitoring of the cluster  
Monitoring operations generate a small amount of traffic.
- Time synchronization for clustering  
Generates standard Network Time Protocol (NTP) traffic.
- Policy Manager configuration changes  
This is not a significant bandwidth consumer.

- Multi-Master Cache  
The amount of traffic depends on the authentication load and other details of the deployment. Cached information is metadata and is not large. This data is replicated only within the Policy Manager zone.
- Guest/Onboard dynamic content proxy requests  
This is essentially a web page and averages approximately 100 KB.
- Guest/Onboard configuration changes  
Only the changes to the database configuration are sent, and this information is typically small in size (approximately 10 KB).

## Round-Trip Time Considerations for Geographically Distributed Clusters

It's important to take the delay between a ClearPass Policy Manager server and a NAD/NAS (a controller or switch) into consideration when building geographically distributed clusters.

In a large geographically dispersed cluster, the worst case round-trip time (RTT) between a NAS /NAD and all potential nodes in the cluster that might handle authentication is a design consideration.

- Aruba recommends that the round-trip time between the NAD/NAS and a ClearPass server should not exceed 600 ms.
- The acceptable delay between cluster nodes is less than 100 ms (RTT less than 200 ms).
- The link bandwidth should be greater than 10 Mbps.

It's possible to configure a NAD/NAS to point at multiple RADIUS servers, either for load balancing or failover.

For example, a NAD/NAS in Paris could point to a ClearPass Policy Manager server in London as a backup RADIUS server. That's not a problem as long as the round-trip time guidelines are adhered to.

## Implementing ClearPass Zones for Geographical Regions

ClearPass zones exist to control the replication of information between nodes in a cluster. Included in this control is the replication of the *Multi-Master Cache* (MMC), which contains the endpoints' run-time state information.

The Multi-Master Cache is replicated across all nodes in a zone—not all nodes in the cluster. If zoning has not been configured, traffic flows between the Publisher and Subscriber nodes, as well as between all the Subscriber nodes in the cluster.

### Run-Time Information

The run-time state information includes:

- Roles and postures of the connected entities
- Connection status of all endpoints running OnGuard
- Machine authentication state
- Session information used for Change of Authorization (CoA)
- Information about which endpoints are on which NAS/NAD

ClearPass uses run-time state information to make policy decisions across multiple transactions.

### When a Cluster Spans WAN Boundaries and Geographic Zones

In a deployment where a cluster spans WAN boundaries and multiple geographic zones, it's not necessary to share run-time state information across all the nodes in the cluster.

For example, endpoints present in one geographical area are not likely to authenticate or be present in another area. It's therefore more efficient from a network usage and processing perspective to restrict the sharing of such run-time state information to a specific geographical area.

Certain cached information is replicated only on the servers within a Policy Manager zone. In a large-scale deployment with multiple geographical areas, multiple zones should be used to reduce the amount of data that needs to be replicated over a wide-area network.

## Zones and the Persistent Agent

A persistent agent attempts to establish communications with a ClearPass server in the same zone; if that is not possible, it contacts a server in another zone.

Zone configurations allow for fairly deterministic control of where the persistent agent will send its health information. At minimum, the agent health information should go to a node in the same zone as the authentication request.

From a design perspective, for large geographically dispersed deployments, the design goal should be for agent health information and authentication requests to be sent to the same cluster node. Targeting authentication requests to a specific node is easily accomplished with NAS configuration.

## Creating Geographical Zones in Policy Manager

You can configure zones in ClearPass Policy Manager to match with the geographical areas in your deployment. You can define multiple zones per cluster. Each zone has a number of ClearPass Policy Manager nodes that share their runtime state.

To create geographical zones in Policy Manager:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.

**Figure 87** Manage Policy Manager Zones Link

The screenshot shows the 'Server Configuration' page under 'Administration > Server Manager'. On the right, a sidebar menu lists various management options. The 'Manage Policy Manager Zones' option is highlighted with a red box. Below the sidebar, a table displays a single server entry: 'Publisher Server: cppm-6.5.6-6.60 [10.17.6.60]'. The table columns are: #, Server Name, Management Port, Data Port, Zone, Insight, Cluster Sync, and Last Sync Time. The 'Server Name' column shows '1. cppm-6.5.6-6.60'. The 'Management Port' column shows '10.'. The 'Zone' column shows 'default'. The 'Cluster Sync' column shows 'Enabled'. At the bottom of the table are buttons for 'Collect Logs', 'Backup', 'Restore', 'Cleanup', 'Shutdown', and 'Reboot'.

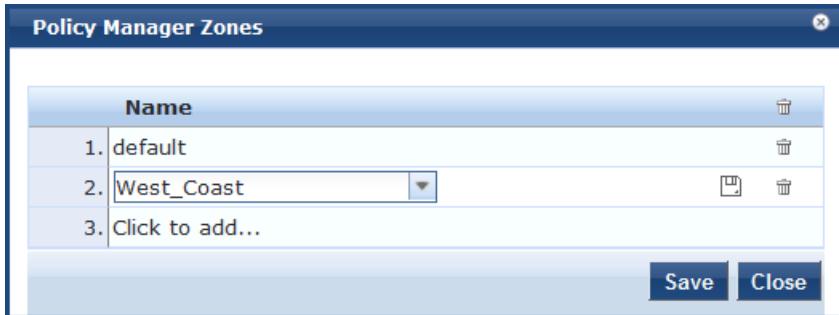
2. Click the **Manage Policy Manager Zones** link.

The Policy Manager Zones dialog opens.

3. Select **Click to add....**

A blank field appears in the dialog.

**Figure 88** Adding a Policy Manager Zone



4. Enter the name of the new Policy Manager zone.
5. To create additional Policy Manager zones, repeat Steps 3 and 4.
6. When finished, click **Save**.

You see the message, "*Policy Manager Zones modified successfully.*"

## Policy Manager Zone Deployment Guidance

Guidance for deploying Policy Manager zones is as follows:

1. In a large-scale deployment, create one Policy Manager zone for each major geographical area of the deployment.
2. To handle RADIUS authentication traffic in each region, configure the region's networking devices with the Policy Manager nodes in the same zone.
3. If additional authentication servers are required for backup, you can specify one or more Policy Manager servers located in a different zone, but Aruba recommends that you deploy remote servers that have the best connection, that is, the lowest latency, highest bandwidth, and highest reliability.
4. There may be cases in which the RADIUS server on the network infrastructure is configured to use remote ClearPass server nodes that are outside of their primary geographic area.

In this scenario, the replication of the runtime states might be relevant. Consider this behavior during the design and deployment of a distributed cluster of ClearPass server nodes.

## About Large Scale Deployments

This section contains the following information:

- [What Is a Large Scale Deployment?](#)
- [Design Guidelines](#)
- [Examples of Customer Cluster Deployments](#)

### What Is a Large Scale Deployment?

Large-scale deployments are defined as those clusters that require the Publisher node to be dedicated to servicing the Subscriber nodes.

This occurs when the volume of configuration changes generated by all the Subscriber nodes in the cluster limits the Publisher node's capacity to handle other important tasks, such as authentication.

Note that not every clustering scenario is a large-scale deployment. ClearPass clustering can also be performed for other reasons, for example, to distribute several ClearPass nodes geographically for policy reasons, or to have an off-site disaster recovery system.

## Design Guidelines

ClearPass cluster design guidelines are as follows:

1. The dedicated Publisher should be a ClearPass C3000 hardware appliance or a ClearPass C3000V virtual appliance that matches the minimum specification for the C3000 virtual appliance:

**Table 24: ClearPass C3000 Virtual Appliance Minimum Specifications**

Component	Specification
CPUs	24 Virtual CPUs
Hard disk	1024 GB hard disk
RAM	64 GB RAM
Switched ports	2 Gigabit virtual switched ports
Functional IOP rating	360 <b>NOTE:</b> For a 40-60 read/write profile for 4K random read/write



For details on the ClearPass hardware and virtual appliances, see [Setting Up the ClearPass Hardware and Virtual Appliances on page 60](#).

2. Configuration changes that should be considered in the context of a large-scale deployment include:
  - Creating, modifying, or deleting a guest account.
  - Issuing or revoking an Onboard certificate.
  - Modifying Policy Manager configuration; for example, adding a network access device, defining a new service, and updating an enforcement profile.
  - Adding new endpoints (including automatically created endpoints) in Policy Manager.
  - Making modifications to guest accounts or endpoint records with a Policy Manager post-authentication profile.

## Examples of Customer Cluster Deployments

This section provides two examples of typical customer cluster deployments.

To find the number of sessions supported by each ClearPass appliance model, refer to the *ClearPass 6.7 Scaling & Ordering Guide*. You can access the *Scaling & Ordering Guide* from the [Aruba Support Center](#) at the following location: **Documentation > Software User & Referenced Guides > ClearPass > Tech Notes > ClearPass 6.7**.

### Authenticating Corporate Users with Guest Access

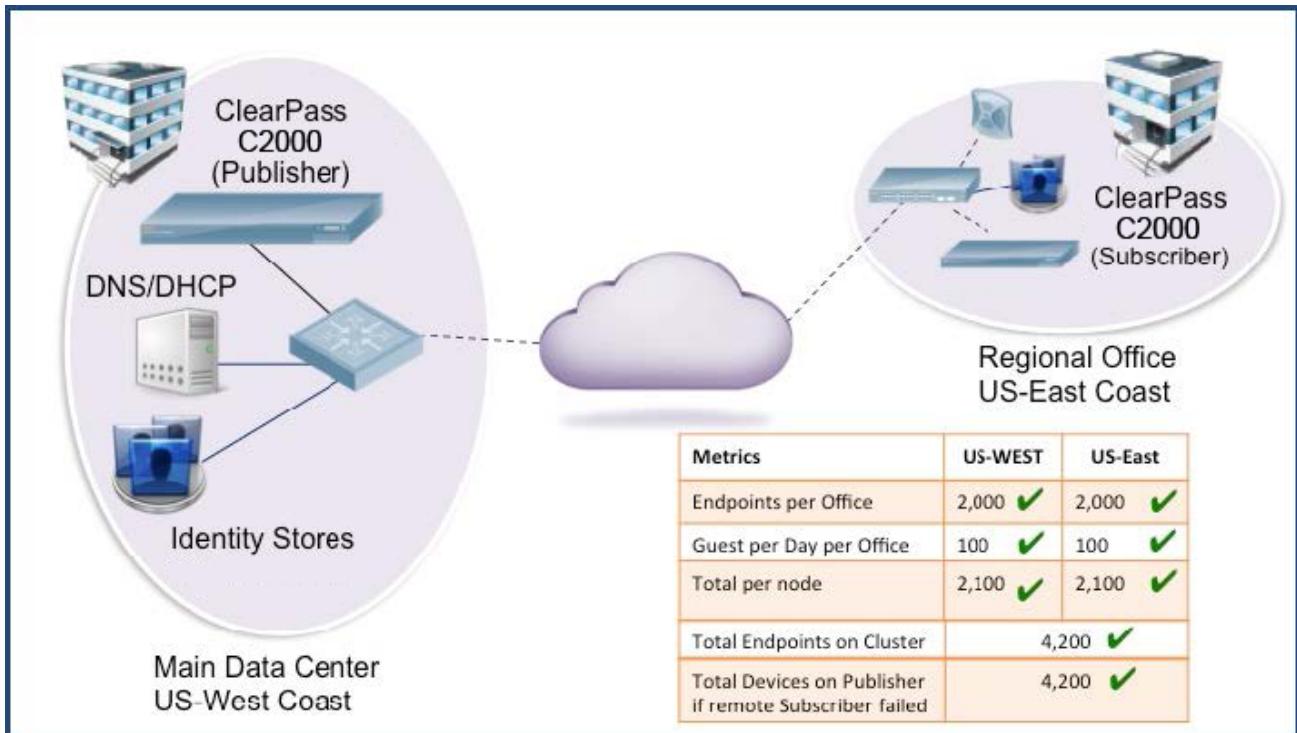
In this example, a cluster of ClearPass C2000 hardware appliances has two nodes—U.S. East Coast and U.S. West Coast (see [Figure 89](#)).

- *US-West* is the Publisher node.
- *US-East* is the Subscriber node.

- Each node handles the authentication traffic for 2,000 corporate endpoints. Each node also registers 100 guests per day.
- There are few configuration updates in the network.

In this example, each node could be used as the backup for the other node. In the event of a node failure, the other node could handle the authentication requirements of all 4,000 endpoints in addition to 200 guest registrations per day.

**Figure 89** Example of a Medium-Scale Cluster Deployment



This fictitious customer example would not be considered a large-scale cluster deployment, for the following reasons:

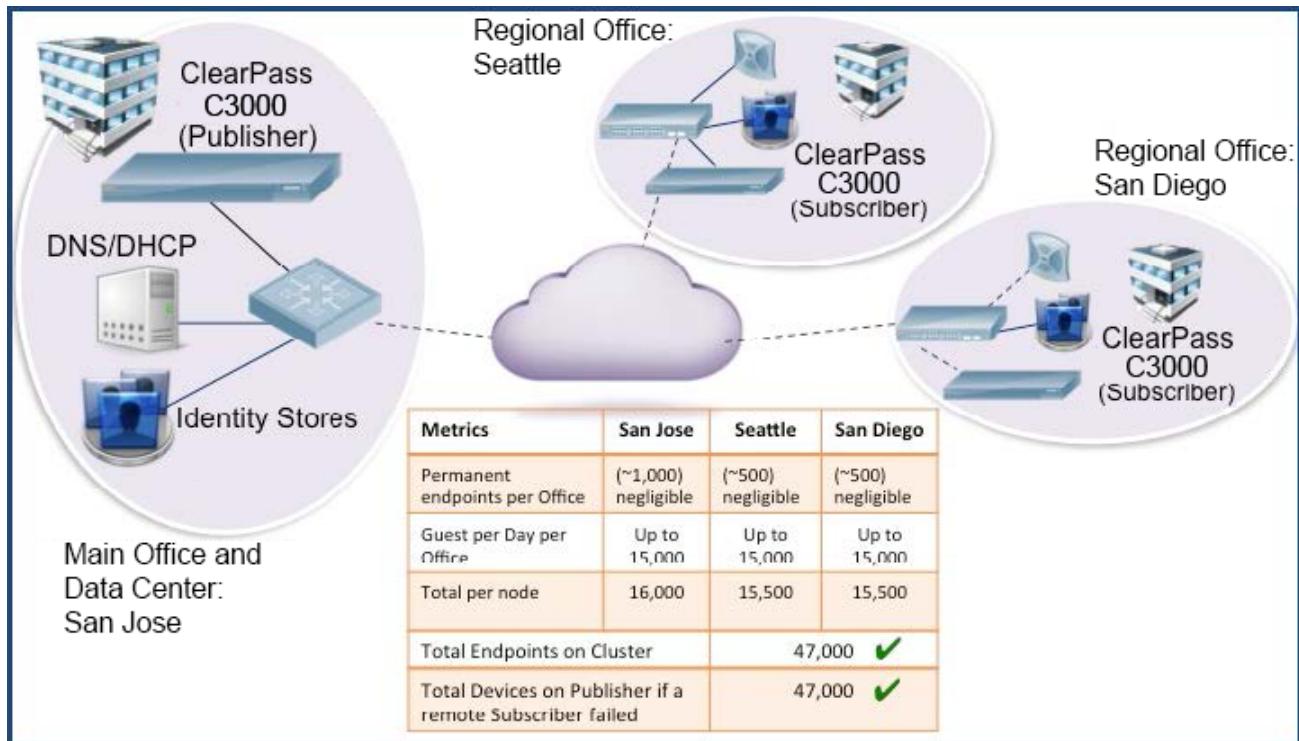
- The additional load on the Publisher due to clustering can be estimated at 100 guest accounts created per day.
- The authentication traffic on the Subscriber node does not impose any additional load on the Publisher and the new endpoints registered (in the order of 100 per day, assuming new guests each day) does also not add any significant load.
- The workload on the Publisher is small and represents a fraction of its capacity.

## Authenticating Conference Center Users

In this example, the cluster has three ClearPass C3000 hardware appliance nodes in the same time-zone (see [Figure 90](#)).

- These nodes are located in San Jose (Publisher), San Diego (Subscriber), and Seattle (Subscriber).
- Each node can register up to 15,000 guests per day, often in short bursts.
- There is constant authentication traffic through the day from the onsite employees and guest.
- On some days, a node may be idle, but there are days where all nodes are busy.

**Figure 90 Example of a Large-Scale Cluster Deployment**



The cluster illustrated in [Figure 90](#) would be considered a large-scale deployment, for the following reasons:

- The maximum potential load on the Publisher due to the Guest account creation process can be estimated at 45,000 guest accounts created per hour (peak rate). That equates to 12.5 account creations per second, with a maximum of 15 accounts created per second.
- This is a significant load on the Publisher.

### Recommendation

In this example, a separate dedicated Publisher node would be recommended: a ClearPass C3000 hardware appliance.

The ClearPass C3000 hardware appliance can handle up to 54,000 guest accounts being created per hour (15 per second), but with bursts of guest traffic that are unpredictable during the peak hours.

With the additional Publisher load of the replication of these accounts to each of the Subscriber nodes, this is an example of a deployment warranting a dedicated Publisher.

# Deploying the Standby Publisher

This section contains the following information:

- [Setting Up the Standby Publisher](#)
- [About the Fail-Over Process](#)
- [Mitigation Strategies](#)
- [Virtual IP Address Considerations](#)
- [Functions Lost When the Publisher Is Down](#)

## Setting Up the Standby Publisher

ClearPass Policy Manager allows you to designate one of the Subscriber nodes in a cluster to be the *Standby Publisher*, thereby providing for that Subscriber node to be automatically promoted to active Publisher status in the event that the Publisher goes out of service. This ensures that any service degradation is limited to an absolute minimum.

During the period when a cluster does not have an active Publisher, some functions across the cluster are not available, such as being able to create guest accounts (for details, see [Functions Lost When the Publisher Is Down](#)).



Before you can designate a ClearPass Policy Manager node as a Standby Publisher, the designated node must be in a cluster.

The Standby Publisher can function as a fully operational Subscriber node. However, in a large cluster deployment, the Publisher and Standby Publisher might need to be dedicated nodes, in which case the Standby Publisher will not be available to handle authentication requests.

If the Standby Publisher is on a different subnet than the Publisher, ensure that a reliable connection between the two subnets is established. This avoids network segmentation and potential data loss from a false failover.

To designate and configure the Standby Publisher:

1. From the node to be designated the Standby Publisher, navigate to **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters > Standby Publisher**.

**Figure 91** Standby Publisher Dialog

Parameter Name	Parameter Value	Default Value
Enable Publisher Failover	FALSE	FALSE
Designated Standby Publisher	0	0
Failover Wait Time	10 minutes	10

2. Configure the **Standby Publisher** parameters as described in [Table 25](#), then click **Save**.

**Table 25: Configuring Standby Publisher Parameters**

Parameter	Action/Description
Enable Publisher Failover	To authorize a node in a cluster to act as a Publisher if the primary Publisher fails, select <b>TRUE</b> . The default value is <b>FALSE</b> .
Designated Standby Publisher	From the drop-down, select the ClearPass server in the cluster that will serve as the Standby Publisher.
Failover Wait Time	Specify the time (in minutes) for which the secondary node waits after the primary node fails before it acquires a virtual IP address. The default failover wait time is 10 minutes, 5 minutes being the minimum value you can select before the Standby Publisher begins to promote itself to an active state. This prevents the secondary node from taking over when the primary node is temporarily unavailable during restart.

## About the Fail-Over Process

The Standby Publisher health-checks the primary Publisher every 60 seconds by making an SQL call to the active Publisher. If this SQL call fails, after ten additional attempts (one per minute), the Standby Publisher begins the process of promoting itself to be the active Publisher node.

The process used to verify the reachability of the remote ClearPass Policy Manager nodes uses an outbound HTTPS call. As noted in [Network Ports That Must Be Enabled on page 117](#), **port 443/TCP** must be open between all the nodes in the cluster. Utilizing this HTTPS health check provides for a more robust and predictable failover process.

When a Publisher failure is detected, the designated Subscriber node is promoted to active Publisher status. The other Subscriber nodes automatically update and replicate their configuration with the new Publisher, which resolves the issue.

## Mitigation Strategies

The recommended mitigation strategies for deploying a Standby Publisher are as follows:

- Use a virtual IP address for the Publisher.  
Doing so reduces the potential for a prolonged service outage while the active Publisher is out of service or promoting the Standby Publisher (for related information, see [Virtual IP Address Considerations](#)).

 When you configure a Standby Publisher and deploy a virtual IP address, the Standby Publisher should be paired with the active Publisher in the VIP group.

- Ensure that the cluster nodes are being monitored.  
Determine if a Publisher node is no longer reachable or not providing service (for example, by SNMP host checking).
- Set up the network access devices (NADs) to point to a primary node, backup node, and a tertiary node.  
Doing so provides for continuity of the RADIUS authentication and accounting traffic until the Standby Publisher transitions to the active state.

## **Virtual IP Address Considerations**

Using a virtual IP address allows for the deployment of a highly available pair of servers. This reduces the amount of down-time in the event of a server failure. If one of the servers in a high-availability pair fails, the other server can take over the virtual IP address and continue providing service to clients. This is particularly useful if the network access server (NAS) devices are processing basic RADIUS authentications to a CPPM node.

The Standby Publisher node cannot take over immediately as the failure may be transient and the minimum time for a Standby Publisher to become active is about eight minutes. This duration is due to five attempts (one per minute) to connect to the active Publisher's database, then about four minutes for the node to promote itself to an active state.

Thus, there will always be a delay before the virtual IP address on the transitioning active Publisher the NAS clients are communicating with is back in service and able to process RADIUS authentication requests.

During this eight-minute window, requests from Subscribers to write to the Publisher's database will fail as there will be no Publisher available that can write to the database.

## **Functions Lost When the Publisher Is Down**

When the active Publisher goes out of service, the following ClearPass Policy Manager functions are temporarily lost:

- AirGroup and MACTrac enrollment
- Certificate creation and revocation
- Certificate revocation list updates
- ClearPass Exchange outbound enforcement
- General ClearPass Policy Manager and ClearPass Guest configuration changes
- ClearPass Guest account creation
- Mobile device management endpoint polling and ingestion
- Onboarding functionality

## **Adding a Subscriber Node to the Publisher**

This section contains the following information:

- [Introduction](#)
- [Using the WebUI to Add a Subscriber Node](#)
- [Using the CLI to Create a Subscriber Node](#)

### **Introduction**

In the Policy Manager cluster environment, the Publisher node acts as the cluster master. 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 hardware or virtual appliance defaults to a Publisher node unless it is made a Subscriber node. You can demote the Publisher to Subscriber status.



---

When the current node is a Subscriber, the **Make Subscriber** link isn't displayed.

---

## Using the WebUI to Add a Subscriber Node

When you make a ClearPass server a Subscriber node in a cluster, keep in mind the following:

- As part of this operation, configuration changes will be blocked on the Publisher during initial cluster sync.
- all application licenses on this server will be removed. To add and activate these licenses, contact Aruba Support (**Administration > Support > Contact Support**).

To add a Subscriber node to a Publisher node via the WebUI:

- Log onto the ClearPass node that you want to make a Subscriber.
- Navigate to **Administration > Server Manager > Server Configuration**.  
The **Server Configuration** page opens.

**Figure 92** *Server Configuration > Make Subscriber Option*

The screenshot shows the 'Server Configuration' page under 'Administration > Server Manager'. On the right, a sidebar menu lists various options: Set Date & Time, Change Cluster Password, Manage Policy Manager Zones, NetEvents Targets, Clear Machine Authentication Cache, Virtual ID Settings, Make Subscriber (which is highlighted with a red box), and Cluster-Wide Parameters. Below the sidebar is a table titled 'Publisher Server: rollback1 [10.10.10.10]'. The table has columns: #, Server Name, Management Port, Data Port, Zone, Insight, Cluster Sync, and Last Sync Time. One row is shown: 1. rollback1, 10., -, default, -, Enabled, -. At the bottom of the table are buttons for Collect Logs, Backup, Restore, Cleanup, Shutdown, and Reboot.

- Click **Make Subscriber**.

The **Add Subscriber Node** dialog opens.

**Figure 93** *Configuring the Subscriber Node*

The 'Add Subscriber Node' dialog box contains fields for 'Publisher IP' and 'Publisher Password'. Below these are two checkboxes: 'Restore the local log database after this operation' and 'Do not back up the existing databases before this operation'. A 'WARNING:' section lists:

- Configuration changes will be blocked on the publisher during initial cluster sync as part of this operation.
- All application licenses on this server will be removed. Please contact support to add and activate these licenses.

At the bottom are 'Save' and 'Cancel' buttons.

- Specify the **Add Subscriber Node** parameters as described in [Table 26](#).

**Table 26: Configuring Add Subscriber Node Parameters**

Parameter	Action/Description
Publisher IP	Enter the Publisher node's IP address.
Publisher Password	Enter the <b>appadmin</b> (CLI) password.
Restore the local log database after this operation	To restore the log database following the addition of a Subscriber node, select this check box.
Do not backup the existing databases before this operation	Select this check box only if you do not require a backup to the existing database.

5. Be sure to note the warnings on this dialog and respond as needed.

6. When finished, click **Save**.

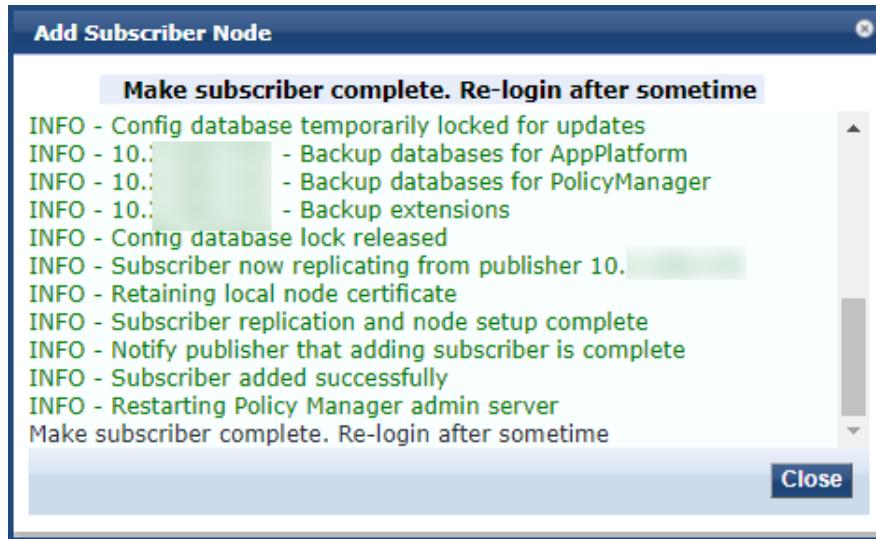
You will see the message: *Adding node as subscriber to <Publisher\_IP\_address>'s cluster.*



The process of adding a node as a Subscriber takes several minutes.

When the process completes, the following messages are displayed:

**Figure 94 Completing Subscriber Setup**



7. Click **Close**.

8. To complete the Subscriber setup, log back into the new Subscriber node.

When you log into the Publisher node or the Subscriber node, the Policy Manager Dashboard presents the updated cluster status:

**Figure 95 Cluster Status: Subscriber Node Added to Publisher**

The screenshot shows the 'Cluster Status' section of the ClearPass Policy Manager interface. It displays a table with columns: Status Host Name, Zone, Server Role, Last Replication, and Status. The table contains three rows:

Status Host Name	Zone	Server Role	Last Replication	Status
avcp671 (10.0.0.1)	default	Publisher	-	OK
rollback1 (10.0.0.2)	default	Subscriber	Feb 16, 2018 13:30:06 PST	Node Down
avcp672 (10.0.0.3)	default	Subscriber	Feb 16, 2018 13:29:56 PST	OK

9. You can also track this process in the Event Viewer (**Monitoring > Event Viewer**) following a successful Subscriber addition, as shown in [Figure 96](#).

**Figure 96 Tracking the Add Node Process in the Event Viewer**

The screenshot shows the 'Event Viewer' interface under 'Monitoring > Event Viewer'. It lists 10 events from a single server. The fourth event, which is the 'AddNode' event for the 'Cluster', is highlighted in yellow and has a blue border. The other events are listed in a standard grid format.

#	Source	Level	Category	Action	Timestamp
1.	Monitor	ERROR	battery		Feb 16, 2018 13:39:15 PST
2.	Policy Manager UI	INFO	Logged in	None	Feb 16, 2018 13:31:21 PST
3.	Monitor	ERROR	battery		Feb 16, 2018 13:24:15 PST
4.	Cluster	INFO	AddNode	Success	Feb 16, 2018 13:21:49 PST
5.	Monitor	ERROR	battery		Feb 16, 2018 13:09:15 PST
6.	Sysmon	ERROR	System	None	Feb 16, 2018 13:05:03 PST
7.	Monitor	ERROR	battery		Feb 16, 2018 12:54:15 PST
8.	Monitor	ERROR	battery		Feb 16, 2018 12:39:15 PST
9.	Monitor	ERROR	battery		Feb 16, 2018 12:24:15 PST
10.	Monitor	ERROR	battery		Feb 16, 2018 12:09:15 PST

10. To view the system event details for the Add Subscriber Node event, click the appropriate Event Viewer item in the list.

The **System Event Details** page for the AddNode event opens.

**Figure 97 Viewing the Add Subscriber Node Event System Event Details**

The screenshot shows the 'System Event Details' dialog box. It contains a table with the following information:

Source	Cluster
Level	INFO
Category	AddNode
Action	Success
Timestamp	Feb 16, 2018 13:21:49 PST
Description	Added subscriber node with management IP=10.0.0.2

## Using the CLI to Create a Subscriber Node

You can perform multiple cluster-related administrative functions from the CLI. The CLI provides additional functionality that cannot be accomplished from the user interface.

In addition to the WebUI, you can use the command-line interface (CLI) to make a Subscriber node.

To use the CLI to make a cluster node a Subscriber:

1. Log in as the **appadmin** user to the ClearPass node using SSH client software (such as PuTTY).
2. Issue the following command:

```
cluster make-subscriber -i [publisher_IP_address]
```

**Table 27: Cluster make-subscriber Command Parameters**

Parameter	Action/Description
-i <publisher_IP_address>	The <b>-i</b> option specifies the Publisher node's IP address.
-l	Use the <b>-l</b> option to restore the local log database after the Make Subscriber operation is complete.
-b	Use the <b>-b</b> option to skip generating a backup before the Make Subscriber operation commences.

After you enter the IP address of the Publisher, you will see the following warning message:

*WARNING: Executing this command will make the current machine subscriber to the publisher host specified. Current configuration and application licenses installed (if any) on this node will be lost when the operation is complete.*

*Do not close the shell or interrupt this command execution.*

3. To confirm that you want to continue, enter **y**.
4. Enter the cluster (**appadmin**) password for the Publisher.

The process to downgrade the node to a Subscriber begins.

## Rejoining a Down Node to the Cluster

This section contains the following information:

- [Introduction](#)
- [Removing a Subscriber Node from the Cluster](#)
- [Rejoining a Disabled Node Back Into the Cluster](#)

### Introduction

When a node loses communication with the cluster for a period greater than 24 hours, the Publisher designates that node as *down*.

To rejoin this node to the cluster requires that you remove the node from the cluster and reset the configuration on the out-of-sync node.

## Removing a Subscriber Node from the Cluster

To remove a Subscriber node from the cluster:

1. From the Publisher node, navigate to **Administration > Server Manager > Server Configuration**.
2. From the **Server Configuration** screen, select the Subscriber you want to remove.

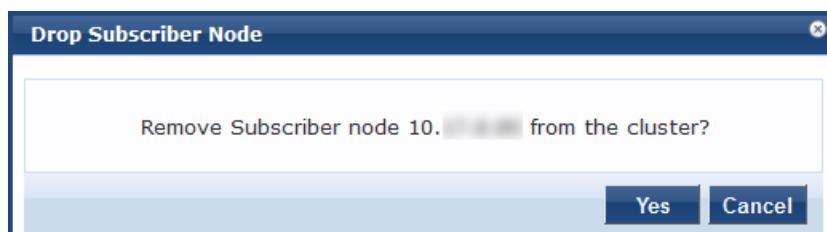
**Figure 98** Selecting the Subscriber Node to Remove

The screenshot shows the 'Server Configuration' screen in the ClearPass Deployment Guide. At the top, there's a breadcrumb trail: Administration > Server Manager > Server Configuration. Below it is a toolbar with several icons: Set Date & Time, Change Cluster Password, Manage Policy Manager Zones, NetEvents Targets, Clear Machine Authentication Cache, Virtual IP Settings, and Cluster-Wide Parameters. The main area displays a table titled 'Publisher Server: avcp671 [10.2.100.176]'. The table has columns: #, Server Name, Management Port, Data Port, Zone, Insight, Cluster Sync, and Last Sync Time. It lists three servers: avcp671, avcp672, and rollback1, all in the default zone and enabled. At the bottom of the table, it says 'Showing 1-3 of 3'. Below the table are several buttons: Collect Logs, Backup, Restore, Cleanup, Shutdown, Reboot, and Drop Subscriber (which is highlighted in yellow). On the right side of the screen, there's a sidebar with some text and icons.

3. Click **Drop Subscriber**.

You are prompted to confirm the drop action.

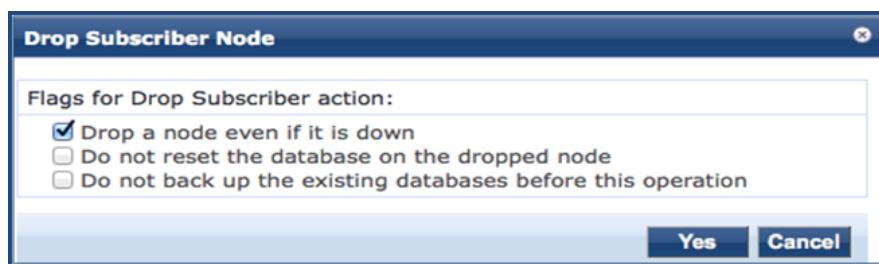
**Figure 99** Confirming the Drop Subscriber Operation



4. To remove the selected Subscriber node, click **Yes** (or press **Cancel** to cancel the operation).

When you proceed, you are presented with a set of options to further refine the Drop Subscriber operation:

**Figure 100** Drop Subscriber Node Confirmation Options



You may optionally choose to enable the following **Drop Subscriber Node** options:

- Drop a node even if it is down.
- Do not reset the database on the dropped node.
- Do not back up the existing databases before this operation.

5. Click the check box for each confirmation option you wish to enable, then click **Yes**.

The **Drop Subscriber Node** status screen is displayed.

6. When the status is complete, click **Close**.

The Subscriber node is removed from the cluster.

## Rejoining a Disabled Node Back Into the Cluster

You can rejoin a cluster node that is currently in the *Disabled* state back into the cluster.

To rejoin a disabled node back into the cluster:

1. Navigate to the **Administration > Server Manager > Server Configuration** page.

[Figure 101](#) shows that one of the Subscribers in the cluster is disabled.

**Figure 101** Server Configuration Page Showing Disabled Cluster Node

The screenshot shows the 'Server Configuration' page under 'Administration > Server Manager'. The left pane lists three servers: vm-65 (disabled), vm-66 (enabled), and vm-69 (enabled). The right pane contains a toolbar with various management options like Set Date & Time, Change Cluster Password, and Manage Policy Manager Zones. Below the toolbar is a table showing the status of each server: Management Port, Data Port, Zone, Profile, Cluster Sync, and Last Sync Time. The 'Cluster Sync' column for vm-65 shows 'Disabled'.

#	Server Name	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	vm-65	[REDACTED]	-	default	Enabled	Disabled	Jan 16, 2015 14:08:28 IST
2.	vm-66	[REDACTED]	-	default	Enabled	Enabled	Jan 16, 2015 14:26:29 IST
3.	vm-69	[REDACTED]	-	default	Enabled	Enabled	-

2. Select the disabled Subscriber node that you want to rejoin to the cluster.

The **Server Configuration > System** dialog opens for the selected node. As shown in [Figure 102](#), the dialog includes the **Join server back to cluster** option.

**Figure 102** Join Server Back to Cluster Option Displayed

The screenshot shows the 'Server Configuration - vm-69 (10. [REDACTED])' dialog. The top right corner features a toolbar with several icons. One icon, 'Join server back to cluster', is highlighted with a red box. Below the toolbar, there are tabs for System, Services Control, Service Parameters, System Monitoring, Network, and FIPS. The System tab is selected. It contains fields for Hostname (vm-69), FQDN, and Policy Manager Zone (default). A 'Manage Policy Manager Zones' link is also present. The toolbar icons include Set Time Zone, Synchronize Cluster Password, Promote To Publisher, and Join server back to cluster.

3. Click **Join server back to cluster**.

A warning message appears, providing the option to promote the current node to Publisher status:

**Figure 103** Option to Promote Disabled Node to Publisher

The screenshot shows the 'Join server back to cluster' dialog box. It asks 'Join server 10. [REDACTED] back to cluster?'. There is a checkbox labeled 'Promote to Publisher?' which is unchecked. A yellow 'WARNING' message at the bottom states: 'WARNING : All data that is not synced from the failed publisher will be lost (like new guest accounts that does not exist in current running publisher.)'. At the bottom are 'Yes' and 'Cancel' buttons.

4. To proceed (without promoting the disabled node to publisher status), click **Yes**.

The progress of the rejoin operation is shown, displaying the log entries for each completed task.

## Deploying ClearPass Insight in a Cluster

This section contains the following information:

- [Introduction](#)
- [ClearPass Insight Placement Considerations](#)
- [When a ClearPass Insight-Enabled Node Is Down](#)
- [Enabling ClearPass Insight](#)

### Introduction

Multiple functions are dependent on ClearPass Insight for them to function, for example, MAC caching. ClearPass Insight must be enabled on at least one node within a cluster.



---

Enabling ClearPass Insight on at least two nodes in the cluster is recommended.

---

As you enable ClearPass Insight on additional nodes in the cluster, CPPM automatically adds these nodes to the ClearPass Insight database authentication source definition.

ClearPass Insight does not replicate data to any other nodes within the cluster—it is an entirely stand-alone database.

### ClearPass Insight Placement Considerations

Having ClearPass Insight enabled on multiple nodes within the cluster provides for a level of resilience, however, you need to carefully consider where you enable ClearPass Insight. For every node where ClearPass Insight is enabled, all the other nodes within the cluster subscribe through *NetEvents* to send data to the ClearPass Insight database.

The amount of data sent to the ClearPass Insight database can be extremely high, and if you use Insight for processing authentication requests within your cluster, where you enable ClearPass Insight is an important design consideration:

- If you are running a large CPPM network in which the subscriber traffic is *not* consuming all the publisher's resources, enable ClearPass Insight on the dedicated publisher and the standby publisher.
- If you are running a very large CPPM network in which the subscriber traffic will consume the publisher's resources, you could enable ClearPass Insight on the dedicated publisher and the standby publisher, but only if both of these nodes are dedicated to cluster operations—the publisher and standby publisher should not be processing authentication requests.
- In a very large-scale deployment, ClearPass Insight should be placed on its own dedicated node. This removes a lot of processing and I/O from the publisher, allowing it to handle the maximum amount of worker traffic.
- ClearPass Insight data is valuable and could be used as part of policy evaluation. If this is the case, Aruba recommends that you enable redundant ClearPass Insight nodes for fault tolerance.
- If the worker traffic sent from the subscriber nodes is expected to fully saturate the capacity of the publisher node, ClearPass Insight should not be enabled on the publisher node. However, if the publisher node has spare capacity, it can be used to support the ClearPass Insight database. However, take care to carefully monitor the publisher node's capacity and performance.

## When a ClearPass Insight-Enabled Node Is Down

When a ClearPass Insight-enabled node in a cluster is down or out-of-sync for more than 30 minutes, the ClearPass Insight node is moved to be the last ClearPass Insight node in the fall-back list. This allows for fail-over to other ClearPass Insight nodes.

When a ClearPass Insight-enabled node is dropped from the cluster, the corresponding node entry in the ClearPass Insight repository is removed.

## Enabling ClearPass Insight

ClearPass Insight is not enabled by default, so you must manually enable it.

To enable ClearPass Insight:

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. From the **Server Configuration** page, select the ClearPass node you want to configure.

The **Server Configuration** dialog opens.

The screenshot shows the 'Server Configuration' dialog for a node named 'avcp671'. The 'System' tab is selected. Key configuration options visible include:

- Hostname: avcp671
- FQDN: (empty)
- Policy Manager Zone: default
- Enable Performance Monitoring Display:  Enable this server for performance monitoring display
- Insight Setting:  Enable Insight  Enable as Insight Master Current Master:-
- Enable Ingress Events Processing:  Enable Ingress Events processing on this server
- Master Server in Zone: Primary master
- Span Port: -- None --

3. To enable the ClearPass Insight reporting tool on this node, select the **Enable Insight** check box.
  - When you enable this check box on a cluster node, the ClearPass Insight Repository configuration is automatically updated to point to the server's management IP address.
  - When you enable this check box for other servers in the cluster, those servers are added as backups for the same authentication source.
  - The order of the primary and backup servers in the ClearPass Insight Repository is the same order in which ClearPass Insight was enabled on those servers.
4. To specify the current cluster node as an Insight Master, click the **Enable as Insight Master** check box. Enabling a cluster node as an Insight Master allows other nodes where Insight has been enabled to subscribe to this node's Insight Report configuration.

In the event that this node fails, the reports will still be produced because all the nodes in the cluster send a copy of their NetEvents data to all the nodes that have ClearPass Insight enabled.
5. When finished with enabling ClearPass Insight and configuring any other elements in the **Server Configuration** dialog, click **Save**.

## Configuring Cluster File-Backup Servers

This section contains the following information:

- [Adding Cluster File-Backup Servers](#)
- [Backing Up Configuration and Access Tracker Log Information](#)

## Adding Cluster File-Backup Servers

To add cluster 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 (SSH File Transfer Protocol) and SCP (Session Control Protocol) protocols.

To configure cluster file-backup servers:

1. Navigate to the **Administration > External Servers > File Backup Servers** page.

The **File Backup Server** page opens.

2. Click the **Add** link (at the top-right).

The **Add File Backup Server** page opens.

**Figure 104** Add File Backup Servers Page

The screenshot shows the 'Add File Backup Server' dialog box. It includes fields for Host, Description, Protocol (set to SFTP), Port (22), Username, Password, Verify Password, Timeout (30), and Remote Directory. A 'ClearPass Servers' section contains a list box with the placeholder '--Select to Add--' and a 'Remove' button. At the bottom are 'Save' and 'Cancel' buttons.

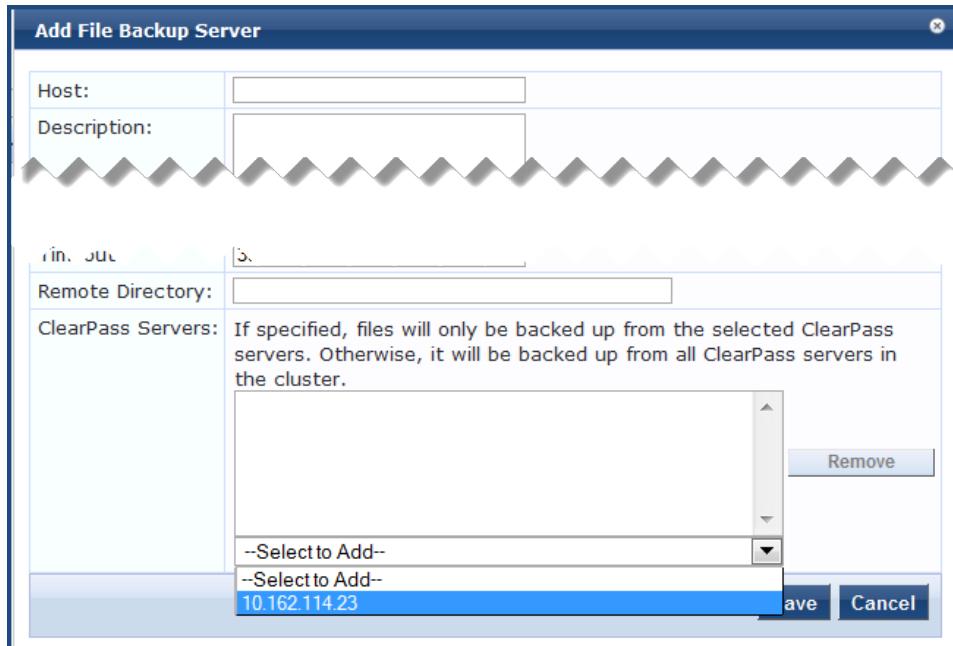
3. Specify the **Add File Backup Server** page parameters as described in the following table.

**Table 28:** Add File Backup Page Server Page Parameters

Parameter	Action/Description
Host	Enter the name or IP address of the host.
Description	Enter the description that provides additional information about the File Backup server.
Protocol	Specify the protocol to be used to upload the generated reports to an external server. Select from the following protocols:

Parameter	Action/Description
	<ul style="list-style-type: none"> <li>SFTP (SSH File Transfer Protocol)</li> <li>SCP (Session Control Protocol)</li> </ul>
Port	Specify the port number. The default port is <b>22</b> .
Username	Enter the user name and password of the host server, then verify the password.
Password	
Timeout	Specify the timeout value in seconds. The default value is <b>30</b> seconds.
Remote Directory	<p>Specify the location where the files are to be copied.  A folder will be automatically created in the file path that you specify based on the selected ClearPass servers in the <b>ClearPass Servers</b> field.</p>
ClearPass Servers	<p>4. From the <b>Select to Add</b> drop-down, select the cluster-file backup server(s) to be backed up.  When you select specific ClearPass servers, files are backed up from the selected ClearPass servers only. Otherwise, the files from all the ClearPass servers in the cluster are backed up.</p>

**Figure 105 Specifying the File Backup Server**



- When finished, click **Save**.

## Backing Up Configuration and Access Tracker Log Information

By default, only cluster configuration information is sent for backup. However, if you need cluster log information to be backed up as well, enter the following change.

To back up both configuration and Access Tracker log information:

1. On the Publisher node, navigate to **Administration > Server Manager > Server Configuration**.
  2. From the **Server Configuration** page, choose **Cluster-Wide Parameters**.
  3. Select the **Database** tab.
- The **Database** page opens.

**Figure 106** Setting the Auto Backup Configuration Options

Parameter Name	Parameter Value	Default Value
Auto backup configuration options	Config	Config
Database user "appexternal" password	*****	
Replication Batch Interval	5 seconds	5
Store Password Hash for MSCHAP authentication	TRUE	TRUE
Store Local User passwords using reversible encryption	TRUE	TRUE

Buttons at the bottom: Restore Defaults, Save, Cancel

4. From the **Auto backup configuration options** drop-down, choose **Config|SessionInfo**.
5. When finished with changes to the cluster-wide parameters, click **Save**.

## Cluster CLI 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 **cluster drop-subscriber** command to remove a specific Subscriber node from the cluster.

#### Syntax

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

[Table 29](#) describes the parameters for the **drop-subscriber** command:

**Table 29: Cluster Drop-Subscriber Command Parameters**

Parameter/Flag	Description
-f	Forces even the nodes that are down to be dropped.
-i <IP address>	Specifies the Management IP address of the node. If this IP address is not specified and the current node is a Subscriber, then Policy Manager drops the current node.
-s	Restricts resetting the database on the dropped node. By default, Policy Manager drops the current node—if it's a Subscriber node—from the cluster.

## Example

The following example removes the Subscriber node with 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 the 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 and add it to the cluster.

## Syntax

```
cluster make-subscriber -b -i <IP address> [-l]
```

[Table 30](#) describes the parameters for the **cluster make-subscriber** command.

**Table 30: Cluster Make-Subscriber Command Parameters**

Parameter/Flag	Description
-b	Generates a backup of the Publisher before you make it a Subscriber in the event the <b>make-subscriber</b> process fails and you need to restore the Publisher.
-i <IP address>	Specifies the publisher IP address. This field is mandatory.
-l	Restores the local log database after this operation. This field is optional.

## Example

The following example 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

The **cluster reset-database** command resets the local database and erases its configuration.



Running this command erases the Policy Manager configuration and resets the database to its default configuration—all the configured data will be lost.

## Syntax and Example

```
cluster reset-database
```



When running this command, do not close the shell or interrupt the command execution.

## cluster set-cluster-passwd

Use the **cluster set-cluster-passwd** command to change the cluster password on all nodes in the cluster. Issue this command from the Publisher node.

### Syntax

```
cluster set-cluster-passwd
```

## Example

The following example changes the cluster password on all the nodes in the cluster:

```
[appadmin]# cluster set-cluster-passwd
cluster set-cluster-passwd
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 and Example

```
[appadmin]# cluster sync-cluster-passwd
```

### Example

The following example changes the local password:

```
[appadmin]# cluster set-local-password  
cluster sync-local-passwd  
Enter Password: college.205  
  
Re-enter Password: college.205
```

# Preparing for Active Directory Authentication

This chapter describes the required steps to integrate ClearPass Policy Manager and Microsoft Active Directory. For some use cases, ClearPass is required to join the Active Directory—802.1X authentication with EAP-PEAP-MSCHAPv2 is one such use case. 802.1X authentication with Active Directory as the primary authentication source is the focus of this chapter.

In other use cases, such as with Captive Portal authentication, joining ClearPass to Active Directory is optional.

This chapter includes the following information:

- [Joining a ClearPass Server to an Active Directory Domain](#)
- [Adding Active Directory as an Authentication Source to ClearPass](#)
- [Obtaining and Installing a Signed Certificate From Active Directory](#)
- [Manually Testing Login Credentials Against Active Directory](#)

## Joining a ClearPass Server to an Active Directory Domain

This section contains the following information:

- [Introduction](#)
- [Synchronizing the Cluster Date and Time with the NTP Server](#)
- [Joining an Active Directory Domain](#)
- [About the Authentication Source and the Authorization Process](#)
- [Manually Configuring Active Directory Password Servers](#)
- [Disassociating a ClearPass Server From an Active Directory Domain](#)

### Introduction

The first task in preparing ClearPass for Active Directory® (AD) authentication via EAP-PEAP-CHAP-v2 is to join the ClearPass server to an Active Directory domain. Joining ClearPass Policy Manager to an Active Directory domain allows you to authenticate users and computers that are members of an Active Directory domain.

Joining ClearPass Policy Manager to an Active Directory domain creates a computer account for the ClearPass node in the Active Directory database. Users can then authenticate to the network using 802.1X and EAP methods, such as PEAP-MSCHAPv2, with their own Active Directory credentials.

When joining an Active Directory domain and doing PEAPv0+MSCHAPv2 authentication, ClearPass negotiates and uses the highest Server Message Block (SMB) protocol version that is supported by the ClearPass server. ClearPass supports SMBv1, v2, and v3.

A one-time procedure to join ClearPass Policy Manager to the domain must be performed from an account that has the ability to join a computer to the domain; if you are unsure whether the administrator account has the ability to do so, check with your Windows administrator.

Why does ClearPass need to join Active Directory to perform EAP-PEAP-MS-CHAPv2 authentication for 802.1x? ClearPass Policy Manager needs to be joined to Active Directory because when performing authentication for a client using EAP-PEAP-MS-CHAPv2, only the password hashes supplied by the user are used to authenticate

against Active Directory. This is done using NT LAN Manager (NTLM) authentication, which requires Active Directory domain membership.

If you need to authenticate users that belong 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 untrusting forests or domains.



You do not need to join ClearPassPolicy Manager to multiple domains belonging to the same Active Directory forest, because a one-way trust relationship exists between these domains. In this case, you should join CPPM to the root domain.

## About the Domain Controller

A *domain* is defined as a logical group of network objects (computers, users, and devices) that share the same Active Directory database.

The *domain controller* is the Microsoft Active Directory server responsible for responding to requests for authentication from users and computer accounts (for example, logging in and checking permissions) within the Windows Server domain. The Active Directory server contains the domain controller.

It's common for an Active Directory domain controller to function as a DNS server. Active Directory domain controllers can also be LDAP servers, as well as perform any number of additional functions that are loaded on the same server.

By default, a domain controller stores one domain directory partition consisting of information about the domain in which it is located, plus the schema and configuration directory partitions for the entire forest.

## Synchronizing the Cluster Date and Time with the NTP Server

Assuming that this ClearPass server has never been joined to the Active Directory domain before, first make sure that the date and time are correct and in sync on both the ClearPass server and the Active Directory domain controller that you will use for the join domain operation.

To synchronize the date and time on the nodes in a cluster with an NTP (Network Time Protocol) server:

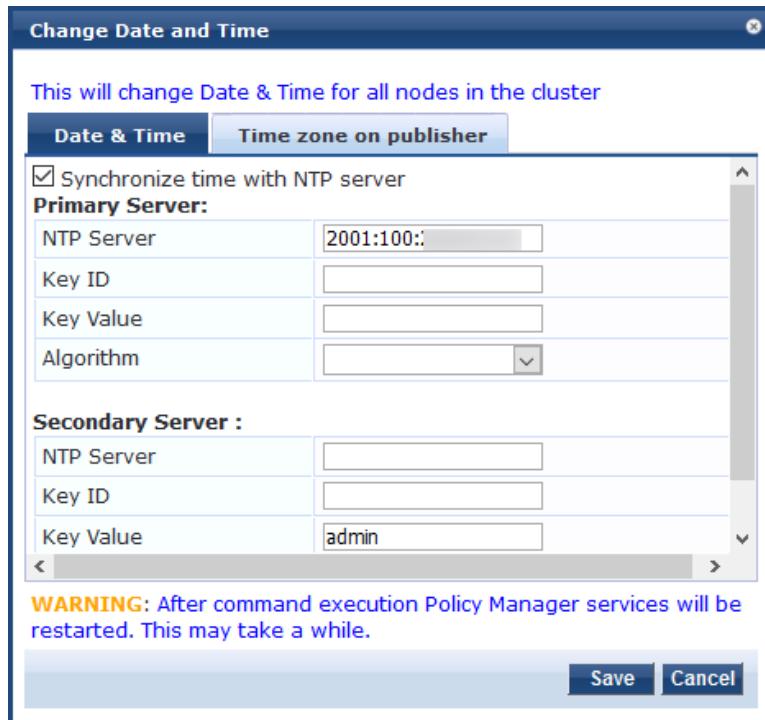


The option to change the date and time for the cluster is available only on the Publisher node. Subscriber nodes in a cluster will synchronize the date and time from the Publisher node.

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 107** Confirming NTP Server Synchronization



4. Specify the **Date & Time** parameters as described in the following table:

**Table 31: Change Date and Time > Date & Time Parameters**

Parameter	Description
Synchronize time with NTP server	<p>To synchronize with a Network Time Protocol (NTP) server, enable this check box (enabled by default).</p> <p><b>NOTE:</b> You can also specify the date and time for the cluster manually by disabling the <b>Synchronize time with NTP server</b> check box and entering the current date and time in the dialog provided:</p>
<b>Primary Server and Secondary Server</b>	
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.

Parameter	Description
Key ID	<p>The <b>Key ID</b> is a number that specifies the index for key values. The <b>Key ID</b> value can be from 1 to 65534 inclusive.</p> <p>For authentication to succeed, typically an NTP client and server have to trust the same key ID and key value pair.</p>
Key Value	<p>The <b>Key Value</b> is a form of shared secret, which both the client and the ClearPass server use for authenticating NTP messages.</p> <p>The <b>Key Value</b> can be:</p> <ul style="list-style-type: none"> <li>● Up to 20-character printable ASCII string</li> <li>● Up to 40-character hex value</li> </ul> <p>When entering an ASCII string for the <b>Key Value</b>, note that it <i>cannot</i> contain the following characters:</p> <ul style="list-style-type: none"> <li>● &amp; (ampersand)</li> <li>● ; (semicolon)</li> <li>● ` (grave accent)</li> <li>●   (pipe)</li> <li>● &lt; (left angle bracket)</li> <li>● &gt; (right angle bracket)</li> <li>● ( (left parenthesis)</li> <li>● ) (right parenthesis)</li> </ul> <p>The <b>Key Value</b> ASCII string must start and end with one of the following characters:</p> <ul style="list-style-type: none"> <li>● - (hyphen)</li> <li>● ' (apostrophe)</li> <li>● " (quotation mark)</li> </ul>
Algorithm	<p>Select one of the following encryption types:</p> <ul style="list-style-type: none"> <li>● SHA</li> <li>● SHA1</li> </ul> <p><b>NOTE:</b> In FIPS mode, only the SHA1 hashing algorithm is supported.</p>

5. Click **Save**.
6. Return to the **Server Configuration** page by clicking **Cancel**.
7. Compare the clock time displayed at the bottom of the ClearPass **Server Configuration** page against the clock time on the Active Directory server.



The maximum allowed clock skew between the ClearPass server and the Active Directory server is **five minutes**.

8. If the time on the two systems doesn't exceed the clock skew limit, then proceed.

## Restarting Services

Once you have saved the **Date & Time** configuration, you must restart 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 108** Restarting Stopped Services

A screenshot of the 'Server Configuration' page under 'Server Manager'. The 'Services Control' tab is selected. A message at the top right says 'Async network services has been stopped'. Below is a table with three rows of service information:

Service Name	Status	Action
1. AirGroup notification service	Stopped	<b>Start</b>
2. Async DB write service	Stopped	<b>Start</b>
3. Async network services	Stopped	<b>Start</b>

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 109** Setting the Time Zone on the Publisher

A screenshot of the 'Change Date and Time' dialog box. The 'Time zone on publisher' tab is selected. It displays a list of time zones for Africa and Asia, with 'Asia/Kolkata(GMT +5:30)' currently selected. A warning message at the bottom states: 'WARNING: After command execution Policy Manager services need to be restarted. This may take a while.' At the bottom are 'Save' and 'Cancel' buttons.

The time zones are listed in alphabetical order.

2. Select the time zone where the Publisher node resides, then click **Save**.



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.

## Joining an Active Directory Domain

You can join ClearPass Policy Manager to an Active Directory (AD) domain to authenticate users and computers that are members of an Active Directory domain. If you join ClearPass to an Active Directory domain, it creates an account for the ClearPass node in the Active Directory database.

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



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 ClearPass is successfully joined. For more information on adding a password server, see [Manually Configuring Active Directory Password Servers](#) below.
- **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 details, see [Disassociating a ClearPass Server From an Active Directory Domain on page 156](#)).

### To Join an Active Directory Domain

To join a ClearPass server to an Active Directory domain:

1. In the **Server Configuration** screen, click the **name of the ClearPass server** that you want to join to the domain.

The **Server Configuration** screen for the selected server opens.

**Figure 110** Join AD Domain Option for Selected ClearPass Server

Administration > Server Manager > Server Configuration - VM-6143

Server Configuration - VM-6143 (10. [REDACTED])

System Services Control Service Parameters System Monitoring Network FIPS

Hostname: VM-6143  
FQDN:  
Policy Manager Zone: default [Manage Policy Manager Zones](#)

Enable Performance Monitoring Display:  Enable this server for performance monitoring display

Insight Setting:  Enable Insight  Enable as Insight Master Current Master:VM-6143(10. [REDACTED])

Enable Ingress Events Processing:  Enable Ingress Events processing on this server

Master Server in Zone: Primary master

Span Port: -- None --

	IPv4	IPv6	Action
Management Port	IP Address: 10.		<a href="#">Configure</a>
	Subnet Mask: 255.255.255.0		<a href="#">Configure</a>
	Default Gateway: 10.		<a href="#">Configure</a>
Data/External Port	IP Address:		<a href="#">Configure</a>
	Subnet Mask:		<a href="#">Configure</a>
	Default Gateway:		<a href="#">Configure</a>
	Primary: 10.		<a href="#">Configure</a>
DNS Settings	Secondary:		<a href="#">Configure</a>
	Tertiary:		<a href="#">Configure</a>
	DNS Caching:	Disabled	<a href="#">Configure</a>
			<a href="#">Configure</a>

**AD Domains:** Policy Manager is not part of any domain. Join to domain here. [Join AD Domain](#)

You can now join the Active Directory domain.



Note that the primary DNS server IP address (as shown in [Figure 110](#)) is also the IP address of the Active Directory domain controller.

2. Click **Join AD Domain**.

The **Join AD Domain** dialog opens.

**Figure 111** Join AD Domain Dialog

Join AD Domain

Enter the FQDN of the controller and the short (NETBIOS) name for the domain:

Domain Controller:

NetBIOS Name:

In case of a controller name conflict:

- Use specified Domain Controller
- Use Domain Controller returned by DNS query
- Fail on conflict

Use default domain admin user [Administrator]

Username: <input type="text"/>
Password: <input type="password"/>

[Save](#) [Cancel](#)

3. Specify the **Join AD Domain** parameters as described in the following table.

**Table 32: Join AD Domain Parameters**

Parameter	Action/Description
Domain Controller	<p>Enter the Fully Qualified Domain Name (FQDN) of the domain controller, then press <b>Tab</b>. The following message is displayed: <i>Trying to determine the NetBIOS name...</i> ClearPass searches for the NetBIOS name for the domain.</p>
NetBIOS name (optional)	<p>Enter the NetBIOS name of the domain.</p> <p>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.</p> <p><b>NOTE:</b> 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 <b>Leave Domain</b> button (which replaces the <b>Join Domain</b> button once you join the domain). After leaving the domain, join again with the correct NetBIOS name.</p>
Domain Controller name conflict	<p>Specify the action to take in the event of a domain controller name conflict.</p> <p>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:</p> <ul style="list-style-type: none"><li>● <b>Use specified Domain Controller:</b> Continue to use the domain controller name that you entered.</li><li>● <b>Use Domain Controller returned by DNS query:</b> Use the domain controller name returned by the DNS query.</li><li>● <b>Fail on conflict:</b> Abort the Join Domain operation.</li></ul>
Use default domain admin user	<p>Check this box to use the Administrator user name to join the domain.</p> <p><b>NOTE:</b> 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 <b>Use default domain admin user [Administrator]</b> check box and 2) enter the Admin username and password in the fields provided.</p>
Username	<p>Enter the user ID of the domain administrator account.</p> <p><b>NOTE:</b> This field is disabled if the <b>Use default domain admin user</b> check box is selected.</p>
Password	<p>Enter the password for the user account that will join ClearPass with the domain (for related information, see <a href="#">Table 33</a>, which displays the characters that are allowed and not allowed for the Active Directory username and password).</p>

**Table 33: Active Directory UserName and Password Characters Allowed**

Field	Characters Allowed	Not Allowed
Username	~ ! @ # \$ % ^ * _ - + = { } , . \ ' " ? /	` & ( )
Password	! @ # \$ % ^ & * ( ) _ - + = { } < , > . ? /	~ ` [ ] \   ; : " ^

[Figure 112](#) shows that ClearPass found the NetBIOS domain name and populated the **NetBIOS Name** field with the correct name.

**Figure 112 Entering the Domain Controller FQDN**

The screenshot shows the 'Join AD Domain' configuration dialog. It includes fields for the Domain Controller (dc1.arubasecurity.net) and NetBIOS Name (ARUBASEURITY). Under 'In case of a controller name conflict', the 'Use specified Domain Controller' radio button is selected. A checked checkbox labeled 'Use default domain admin user [Administrator]' is present. Below these are fields for 'Username' and 'Password', both currently empty. At the bottom are 'Save' and 'Cancel' buttons.

**4. In case of a controller name conflict:**

- Use specified Domain Controller:** Accept the default setting.
- Use default domain admin user [Administrator]:** Accept the default setting.

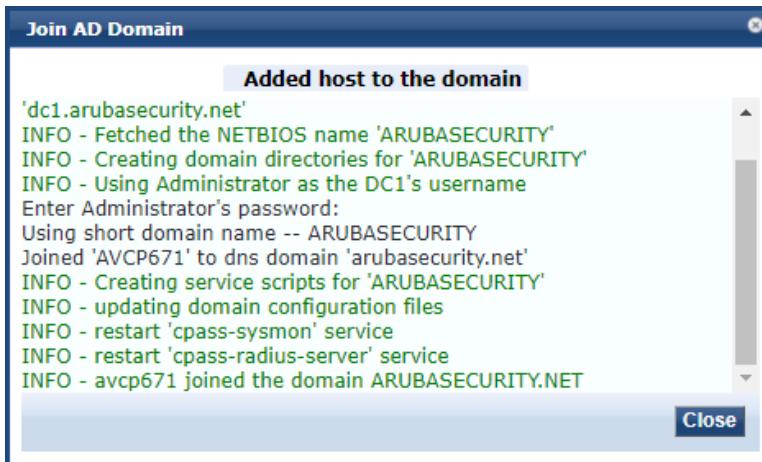
In a production environment, it is likely that an Administrative username that has permissions to join machines to the domain would be used for the default domain admin user. In that case, 1) disable (uncheck) the **Use default domain admin user [Administrator]** check box and 2) enter the Administrative username and password in the fields provided.

- Password:** Enter the password for the user account that will join ClearPass with the domain.
- 5. Click Save.**
- The **Join AD Domain** 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."



**Figure 113** ClearPass Server Added to the Active Directory Domain



The **Join AD Domain** status screen indicates that the services have restarted. As shown in [Figure 113](#), the final INFO line states that the selected ClearPass server joined the domain.

6. Click **Close**.

You return to the **Server Configuration** page, and it now shows that the ClearPass server is joined to the domain.

**Figure 114** ClearPass Server Joined to Domain

The screenshot shows the 'Server Configuration' page for 'avcp671'. The 'System' tab is selected. In the 'AD Domains' section, there is a table with one row:

Domain Controller	NetBIOS Name	Password Servers	Action
1. ARUBASEURITY.NET	ARUBASEURITY	-	<a href="#">Join AD Domain</a> <a href="#">Leave AD Domain</a>

A red box highlights the first row of the table. At the bottom of the page are buttons for [Back to Server Configuration](#), [Save](#), and [Cancel](#).

Now that the ClearPass Policy Manager server has joined the domain, the server can authenticate users with Active Directory.

## About the Authentication Source and the Authorization Process

During the NT LAN Manager authentication process, ClearPass queries Active Directory for a suitable domain controller to use to handle the authentication.

Please note that when used with 802.1x EAP-PEAP-MSCHAPv2 services, the authentication process is separate from the Active Directory authentication source in ClearPass, which in this context only handles authorization.

Optionally, you can configure a list of domain controllers to be used for MSCHAPv2 authentication, as described in the next section, [Manually Configuring Active Directory Password Servers](#).

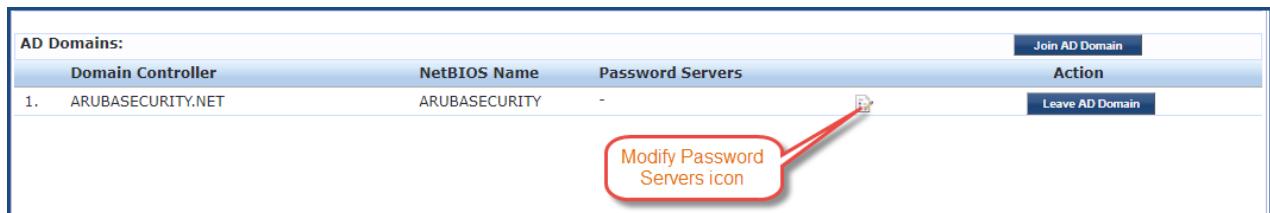
If you do not specify this list of domain controllers, all available domain controllers obtained from DNS will be used for authentication.

## Manually Configuring Active Directory Password Servers

To manually specify Active Directory domain controllers for authentication:

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. Select the ClearPass server name.  
The **Server Configuration** page for the selected server opens to the **System** tab.
3. Click the **Modify Password Servers** icon (located at the bottom of the **System** page).

**Figure 115** Location of Modify Password Servers Icon



The **Configure AD Passwords Servers** screen opens.

**Figure 116** Configuring Active Directory Password Servers

Domain Controller:	ARUBASECURITY.NET
NetBIOS Name:	ARUBASESECURITY
Password Servers:	ad3dc1.ad3dc1.arubasecurity.net

4. In the **Password Servers** text box, enter the names of the domain controllers that will be used for authentication (one entry per line).
5. When finished, click **Save**.

## Disassociating a ClearPass Server From an Active Directory Domain

When leaving an Active Directory domain, ClearPass uses the supplied credentials to remove the "Computer Account" from Active Directory before removing its own relationship with that AD domain that exists on ClearPass itself.

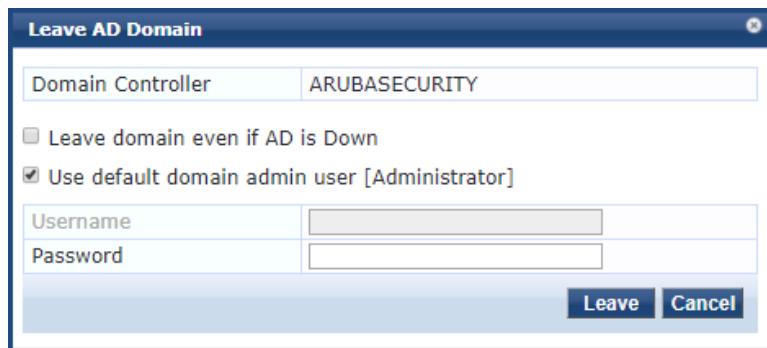
If a ClearPass Policy Manager server is already part of multiple Active Directory domains, follow this procedure to disassociate this ClearPass appliance from an Active Directory domain.

To disassociate a ClearPass server from an Active Directory domain:

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. Select the name of the ClearPass server that you want to disassociate from the domain.
3. Click **Leave AD Domain**.

The **Leave AD Domain** dialog opens.

**Figure 117** Leave AD Domain Dialog



4. Specify the **Leave AD Domain** parameters as described in the following table.

**Table 34: Leave AD Domain Parameters**

Parameter	Action/Description
Leave domain even if AD is Down	When you enable <b>Leave domain even if AD is Down</b> , ClearPass tries to delete the Computer Account from Active Directory, but instead of stopping the leave process if Active Directory is unreachable, ClearPass removes its own links to Active Directory.  In that event, the Active Directory administrator should manually remove the Computer Account.
Use default domain admin user [Administrator]	This option allows you to use either the <i>administrator</i> user account or another account in Active Directory that has the same privileges. This option is enabled by default.  <b>NOTE:</b> The Administrator account doesn't have to be the same account that is used to join the server to the domain—it only has to be an account that has permissions to do this operation.
Password	Enter the Administrator account password.

5. Click **Leave**.

The **Leave AD Domain** status screen appears, with the heading message: "Removing host from the AD domain."

When the process is complete, the status screen displays the message: "Removed host from the domain."

6. Click **Close**.

When you return to the **Server Configuration > System** page, the ClearPass server is no longer listed in the AD Domains section.

7. Click **Save**.

## Adding Active Directory as an Authentication Source to ClearPass

This section includes the following information:

- [About Authorization](#)
- [User Objects](#)
- [About the Bind Operation](#)
- [Adding Active Directory as an Authentication Source](#)

After you have joined ClearPass to the domain, add an authentication source to ClearPass in order to process authentication and authorization against this Active Directory.

This section describes how to add the Active Directory server as an authentication source in ClearPass. This allows ClearPass Policy Manager to communicate with Active Directory in order to accomplish authentication and authorization operations.

If you are using EAP-PEAP-MS-CHAPv2, you must join ClearPass Policy Manager to the Active Directory domain. Joining the Active Directory domain is necessary in order for ClearPass Policy Manager to gain access to the user credential information stored in the Active Directory.



---

If you are using EAP-TLS for checking client certificates, you don't need to join the ClearPass server to the domain.

---

### About Authorization

Authorization is the function of specifying access rights to resources related to information security and computer security in general and to access control in particular. In functional terms, "to authorize" is to define an access policy.

In the context of 802.1X authentication, authorization is accomplished using LDAP (Lightweight Directory Access Protocol). LDAP is a protocol for accessing directories. It offers means to search, retrieve, and manipulate directory content and also provides access to a rich set of security functions.

LDAP provides the ability to locate organizations, individuals, and other resources, such as files and devices in a network, whether on the Internet or on a corporate intranet.



---

When authenticating users via EAP-PEAP-MSCHAPv2 to Active Directory, the authentication source created in ClearPass only serves for authorization and not authentication. When authenticating users via Captive Portal, the authentication source created in ClearPass serves both authorization and authentication functions.

---

### User Objects

The directory is simply a list of objects. One of those types of objects is a "user" object, and that user object has a number of different attributes, such as last name, first name, group membership, phone number, and so on. There is a default set of attributes, however, the list of user attributes is customizable.

An authentication source of type Active Directory is essentially an LDAP query that ClearPass runs. When a user is authenticating, they give ClearPass their username. After authentication is successfully completed, ClearPass takes the username and, using Active Directory via LDAP, looks up the user and finds all the LDAP attributes pertaining to that user.

## About the Bind Operation

The Bind operation allows authentication information to be exchanged between the client and server to establish a new authorization state.

In the Active Directory context, *bind* is a term that indicates authenticating to an LDAP server, which Active Directory must do before it can run any queries against the LDAP server.

Active Directory must provide credentials to prove to the LDAP server that it is authorized to make queries against it. Only entities and devices that have an account can make queries against Active Directory.

## Adding Active Directory as an Authentication Source

This procedure creates an enforcement policy that is based on information that Active Directory has about users in the domain.

### Group Membership

The most commonly applied user attribute is *group membership*. In Active Directory, you can define groups and put users into the groups you define. For example, a college might have groups for students, faculty, and contractors.

For example, the enforcement policy can dictate that students are given a limited level of access to the network, whereas members of the faculty are typically given a higher level of access to the network, though faculty access would be less network access than that granted to network administrators and operators.

Active Directory needs to know which group each user who is trying to authenticate is a member of. This allows ClearPass to do *enforcement*, which is the process of specifying what each user will be allowed to do on the network.

After authentication takes place, there are usually additional enforcement details provided to the controller, such as VLAN assignment and user membership.

To add Active Directory as an authentication source:

1. In ClearPass Policy Manager, navigate to **Configuration > Authentication > Sources**.

The following page opens:

**Figure 118** Authentication Sources Page

Authentication Sources			
#	Name	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	Bangalore-AD	Active Directory	
3.	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
4.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
5.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
6.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
7.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
8.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
9.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
10.	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database

- Click the **Add** link.

The **Add Authentication Sources > General** page opens.

## General Page

**Figure 119** Add Active Directory Authentication Sources > General Page

Authentication Sources	
	General Primary Attributes Summary
Name:	Aruba Security AD
Description:	Authentication source to be used for enforcement policy to define access to the ArubaOS switch
Type:	Active Directory
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes
Authorization Sources:	<ul style="list-style-type: none"> <li>-- Select --</li> </ul> <div style="text-align: right;"> <input type="button" value="Remove"/> <input type="button" value="View Details"/> </div>
Server Timeout:	10 seconds
Cache Timeout:	36000 seconds
Backup Servers Priority:	<ul style="list-style-type: none"> <li>-- Select --</li> </ul> <div style="text-align: right;"> <input type="button" value="Move Up"/> <input type="button" value="Move Down"/>   <input type="button" value="Add Backup"/> <input type="button" value="Remove"/> </div>

- Enter the values for **Add Authentication Sources** parameters as described in [Table 35](#).

**Table 35:** General Parameters for Adding an AD Authentication Source

Parameter	Action/Description
Name	<p>Enter the name of the Active Directory authentication source.</p> <p>The name of this authentication source will be needed when you create the enforcement policy (see <a href="#">Switch Management Using TACACS+ on page 196</a>) and the role-mapping policy.</p> <p><b>NOTE:</b> In this example, we assign the name of the Active Directory authentication source as "Aruba Security AD." Assign a name to the authentication source that is appropriate for your network or installation.</p>
Description	Provide the additional information that helps to identify the Active Directory authentication source.
Type	If not already selected, select <b>Active Directory</b> .
Use for Authorization	When <i>Use for Authorization</i> is enabled, ClearPass can use this authentication source to fetch role-mapping attributes. This option is enabled by default.
Authorization Sources	<p>Specifies additional sources from which role-mapping attributes may be fetched.</p> <p>Select a previously configured authentication source from the drop-down list.</p> <ul style="list-style-type: none"> <li>• To add authentication source to the list of authorization sources, click <b>Add</b>.</li> </ul>

Parameter	Action/Description
	<ul style="list-style-type: none"> <li>To remove the authentication source from the list, click <b>Remove</b>.</li> </ul> <p>If Policy Manager authenticates the user or device from this authentication source, it also fetches role mapping attributes from these additional authorization sources.</p>
Server Timeout	<p>Specifies the duration in number of seconds that Policy Manager waits before considering this server unreachable.</p> <p>If multiple backup servers are available, then this value indicates the duration in number of seconds that Policy Manager waits before attempting to fail over from the primary to the backup servers in the order in which they are configured.</p>
Cache Timeout	Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the duration in number of seconds for which the attributes are cached.
Backup Servers Priority	<ol style="list-style-type: none"> <li>To add a backup server, click <b>Add Backup</b>. The <b>Backup 1</b> tab appears. The <b>Primary</b> page parameters are prepopulated in the <b>Backup 1</b> page.</li> <li>To complete the configuration for the backup server, specify the hostname for the backup server.</li> <li>To remove a backup server, select the server name and click <b>Remove</b>.</li> <li>To change the server priority of the backup servers, select <b>Move Up</b> or <b>Move Down</b>.</li> </ol> <p>The server priority is the order in which Policy Manager attempts to connect to the backup servers when the primary server is unreachable.</p> <p><b>NOTE:</b> Aruba recommends setting up one or more backup servers.</p>

3. When satisfied with these settings, click **Next**.

The **Add Authentication Sources > Primary** page opens.

## Primary Page

**Figure 120 Add Active Directory Authentication Sources > Primary Page**

Configuration > Authentication > Sources > Add  
Authentication Sources

General	Primary	Attributes	Summary																											
<b>Connection Details</b> <table border="1"> <tr> <td>Hostname:</td> <td>ad1dc2</td> </tr> <tr> <td>Connection Security:</td> <td>AD over SSL</td> </tr> <tr> <td>Port:</td> <td>636 (For secure connection, use 636)</td> </tr> <tr> <td>Verify Server Certificate:</td> <td><input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection</td> </tr> <tr> <td>Bind DN:</td> <td>dc=arubasecurity,dc=net (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)</td> </tr> <tr> <td>Bind Password:</td> <td>*****</td> </tr> <tr> <td>NetBIOS Domain Name:</td> <td></td> </tr> <tr> <td>Base DN:</td> <td>dc=arubasecurity,dc=net</td> <td><a href="#">Search Base Dn</a></td> </tr> <tr> <td>Search Scope:</td> <td>SubTree Search</td> </tr> <tr> <td>LDAP Referrals:</td> <td><input type="checkbox"/> Follow referrals</td> </tr> <tr> <td>Bind User:</td> <td><input checked="" type="checkbox"/> Allow bind using user password</td> </tr> <tr> <td>User Certificate:</td> <td>userCertificate</td> </tr> <tr> <td>Always use NETBIOS name:</td> <td><input type="checkbox"/> Enable to always use NETBIOS name instead of the domain part in username for authentication</td> </tr> </table>				Hostname:	ad1dc2	Connection Security:	AD over SSL	Port:	636 (For secure connection, use 636)	Verify Server Certificate:	<input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection	Bind DN:	dc=arubasecurity,dc=net (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)	Bind Password:	*****	NetBIOS Domain Name:		Base DN:	dc=arubasecurity,dc=net	<a href="#">Search Base Dn</a>	Search Scope:	SubTree Search	LDAP Referrals:	<input type="checkbox"/> Follow referrals	Bind User:	<input checked="" type="checkbox"/> Allow bind using user password	User Certificate:	userCertificate	Always use NETBIOS name:	<input type="checkbox"/> Enable to always use NETBIOS name instead of the domain part in username for authentication
Hostname:	ad1dc2																													
Connection Security:	AD over SSL																													
Port:	636 (For secure connection, use 636)																													
Verify Server Certificate:	<input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection																													
Bind DN:	dc=arubasecurity,dc=net (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)																													
Bind Password:	*****																													
NetBIOS Domain Name:																														
Base DN:	dc=arubasecurity,dc=net	<a href="#">Search Base Dn</a>																												
Search Scope:	SubTree Search																													
LDAP Referrals:	<input type="checkbox"/> Follow referrals																													
Bind User:	<input checked="" type="checkbox"/> Allow bind using user password																													
User Certificate:	userCertificate																													
Always use NETBIOS name:	<input type="checkbox"/> Enable to always use NETBIOS name instead of the domain part in username for authentication																													

4. Enter the information for each of the required parameters as described in [Table 36](#).

**Table 36: Primary Parameters for an Active Directory Authentication Source**

Parameter	Action/Description
Hostname	<p>Enter the name or IP address of the Active Directory server you're going to use for authentication.</p> <p>The host name entered here must be an LDAP server (note that most domain controllers are also LDAP servers). ClearPass uses LDAP to talk to the domain controller.</p>
Connection Security	<p>Set <b>Connection Security</b> to: <b>AD over SSL</b>.</p> <p>This enables the secure sockets layer (SSL) cryptographic protocol to connect to your Active Directory. Selecting <b>AD over SSL</b> automatically populates the <i>Port</i> field to <b>636</b>.</p> <p><b>NOTE:</b> 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 <b>636</b>.</p> <p><b>NOTE:</b> To ensure successful authentication, be sure to add the CA certificate of the Active Directory/LDAP server to the Certificate Trust List. For more information, refer to <a href="#">Importing the Root CA Files to the Certificate Trust List</a>.</p>
Port	<p>Specify the TCP port at which the Active Directory server is listening for connections.</p> <p>For a single domain Active Directory Domain Service:</p> <ul style="list-style-type: none"> <li>• Default port for LDAP: <b>389</b></li> <li>• Default port for LDAP over SSL: <b>636</b></li> </ul> <p>When you set the <i>Connection Security</i> field to <b>AD over SSL</b>, this port is automatically set to <b>636</b>.</p> <p>For a multi-domain Active Directory Domain Service (AD DS) forest, the default ports for the global catalog are:</p> <ul style="list-style-type: none"> <li>• Default port without SSL: <b>3268</b></li> <li>• Default port with SSL: <b>3269</b></li> </ul>
Verify Server Certificate	Enable this option to verify the Server Certificate for a secure connection.
Bind DN	<p>Enter the Distinguished Name of the node in your directory tree from which to start searching for records. This is a required parameter.</p> <p>The Bind DN text box specifies the full distinguished name (DN), including common name (CN), of an Active Directory user account that has privileges to search for users (usually the Administrator account). For example:</p> <p>CN=Administrator,CN=Users,DC=mycompany,DC=com</p> <p><b>NOTE:</b> You may need to get the Bind DN from the Active Directory administrator. This user account must have at least domain user privileges.</p> <p>The Bind DN user, such as Administrator, is the username associated with the Bind DN user account.</p>

Parameter	Action/Description
	<ul style="list-style-type: none"> <li>For a single domain Active Directory Domain Service, the Bind DN entry must be located in the same branch and below the Base DN.</li> <li>For a multi-domain Active Directory Domain Service (AD DS) forest, because you leave the Base DN text box empty, the restrictions that apply for a single domain do not apply for a multi-domain forest.</li> </ul> <p>ClearPass fills in the domain portion of the Bind DN.</p> <p>5. Specify the username.</p> <p>ClearPass also populates the <i>Base DN</i>, and the <i>NetBIOS Domain Name</i> fields.</p> <p>For related information, see <a href="#">About the Bind Operation</a>.</p>
Bind Password	<p>This is the text box for the Active Directory password for the account that can search for users. This is a required parameter.</p> <p>Enter the <b>Bind Password</b>.</p> <p><b>NOTE:</b> The Bind password is the same password used in association with the Bind DN user account.</p>
NetBIOS Domain Name	<p>This field is automatically populated.</p>
Base DN	<ul style="list-style-type: none"> <li>For a single domain Active Directory Domain Service, this is the text box for the Distinguished Name (DN) of the starting point for directory server searches. This is a required parameter.</li> </ul> <p>For example: DC=mycompany,DC=com</p> <p>Active Directory starts from this DN to create master lists from which you can later filter out individual users and groups.</p> <p><b>NOTE:</b> The Base DN value that is automatically populated in this instance is <i>not</i> the best practice Base DN value.</p> <p>Aruba recommends that you narrow down the Base DN as far as possible to reduce the load on the Active Directory/LDAP server. For example, if all your users are in the AD Users and Computer Users folder, then set the Base DN to search in that folder.</p> <p>To browse the LDAP directory hierarchy:</p> <ol style="list-style-type: none"> <li>Click <b>Search Base DN</b>. The LDAP browser opens.</li> <li>Navigate to the DN you want to use as the Base DN.</li> <li>Click the appropriate node in the tree structure to select it as a Base DN.</li> <li>For a multi-domain Active Directory Domain Service (AD DS) forest, the appropriate action is to leave the Base DN text box blank.</li> </ol> <p><b>NOTE:</b> This is also one way to test the connectivity to your Active Directory directory. If the values entered for the primary server attributes are correct, you should be able to browse the directory hierarchy by clicking <b>Search Base DN</b>.</p>
Search Scope	<p>Search scope is related to the Base DN. The search scope defines how Active Directory will search for your objects.</p> <p>Specify the search scope you wish to apply.</p> <ul style="list-style-type: none"> <li>Subtree Search: Searches every object and sub-object in the LDAP directory.</li> </ul>

Parameter	Action/Description
	<ul style="list-style-type: none"> <li>One-Level Search: Looks directly under the Base DN.</li> <li>Base Object: Searches any object under the Base DN.</li> </ul>
LDAP Referrals	Aruba recommends <i>not</i> enabling the "Follow Referrals" check box. This function directs the LDAP server to find a specific user in its tree, but it's possible for the user to be included on another LDAP server, which can cause a search loop.
Bind User	This option allows the bind operation using a password. The <b>Allow bind using user password</b> check box is enabled by default.
User Certificate	Leave the value that is automatically populated in this field as the default unless your Active Directory administrator has a different attribute for storing the user certificate.
Always use NetBIOS name	Enable this option only if you want to use the value specified in the <i>NetBIOS Domain Name</i> field to authenticate the user instead of using the domain name present in the User Name RADIUS attribute.

4. When satisfied with the **Add Authentication Sources Primary** page settings, click **Next**.

The **Add Active Directory Authentication Sources > Attributes** page opens.

### Active Directory > Attributes Page

The **Attributes** page defines the Active Directory or LDAP Directory query filters and the attributes to be fetched by using those filters.

**Figure 121 Add Active Directory Authentication Sources > Attributes Page**

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

5. Click **Save**.

You return to the **Authentication Sources** page where the new authentication source is now listed. The following message is displayed:

*Authentication source <authentication source name> added*

# Obtaining and Installing a Signed Certificate From Active Directory

This section describes how to obtain and install a signed server certificate from Active Directory for 802.1X authentication. This section contains the following information:

- [About Certificates in ClearPass Deployments](#)
- [Tasks to Obtain a Signed Certificate from Active Directory](#)
- [Creating a Certificate Signing Request](#)
- [Importing the Root CA Files to the Certificate Trust List](#)
- [Obtaining a Signed Certificate from Active Directory](#)
- [Importing a Server Certificate into ClearPass](#)

## About Certificates in ClearPass Deployments

A certificate is a file that makes it possible for network devices to communicate with each other securely. For example, in ClearPass deployments, certificates are provided for all devices involved in authentication, such as client laptops, smart phones, Mobility controllers, Mobility Access Switches, ArubaOS switches, ClearPass Policy Manager servers, and so on.

How do certificates help you communicate securely? It does this in two ways:

- Certificates help devices verify the identity of other devices.
- Certificates enable devices to use encryption to securely communicate with each other.

When a certificate is created, two keys are generated:

- **Private key**

The private key is always stored securely and never sent out. If the private key is compromised, the entire security framework established by the certificate is compromised.

- **Public key**

The public key contains important information about the certificate owner. The public key is inside the file that is sent to all devices that wish to communicate with the certificate owner. This file contains additional information about the identity of the certificate owner's device.

Public and private key pairs are generated so that any data encrypted by one of these keys can only be decrypted by the other corresponding key.

Any data encrypted by the private key can only be decrypted by the corresponding public key. Conversely, any data encrypted by the public key can only be decrypted by the corresponding private key.

## When Certificate Usage Is Necessary

There are three common situations in which certificates are necessary in ClearPass deployments:

- When using HTTPS to manage network devices such as mobility controllers, mobility access switches, ArubaOS switches or ClearPass servers.
- During captive portal authentication.
- When doing 802.1X authentication.

## How 802.1X Authentication Uses Server Certificates

When an employee attempts to log into his laptop, the EAP-PEAP authentication process begins:

1. The ClearPass Policy Manager server sends the server certificate to the employee's device.
2. The employee sends his encrypted username and password to the server.

3. The server verifies the employee's credentials, and the employee is connected to the network.

## Using Both Client and Server Certificates

There is a potential problem in this authentication sequence—the employee verified the server's identity, but the server didn't verify the employee's identity. It is possible that the user stole the username and password from another employee and is using these stolen credentials on his own device.

This problem can be solved by using both a client certificate and a server certificate. Because EAP-TLS authentication employs both server and client certificates, when the employee begins authentication, the ClearPass server sends the server certificate to the employee's laptop. The employee's laptop then sends the client certificate to the server.

Both the client and the server can then verify the identity of the other party and are ready to proceed: The employee sends the encrypted username and password to the server, the server verifies the employee's credentials, and the employee is connected to the network. This access process is secure.

## Tasks to Obtain a Signed Certificate from Active Directory

The tasks to obtain a signed certificate from Active Directory are as follows:

1. Create a Certificate Signing Request.
2. Import the root Certificate Authority file to the Certificate Trust List.
3. Obtain a signed certificate from Active Directory.
4. Import the server certificate into the ClearPass Policy Manager server.

These tasks are described in the following sections.

## Creating a Certificate Signing Request

This task creates a Certificate Signing Request to be signed by a Certificate Authority (CA).

[Figure 122](#) shows an example of the **Create Certificate Signing Request** page, followed by descriptions of each parameter (see [Table 37](#)).

To create a Certificate Signing Request:

1. In ClearPass, navigate to **Administration > Certificates > Server Certificates**.
2. Select the **Create Certificate Signing Request** link.

**Figure 122** *Create Certificate Signing Request Dialog*

Create Certificate Signing Request	
Common Name (CN):	665_PTU_HYPV
Organization (O):	Acme Widgets
Organizational Unit (OU):	Design
Location (L):	Boston
State (ST):	MA
Country (C):	US
Subject Alternate Name (SAN):	email:admin@acmewidgets.com
Private Key Password:	*****
Verify Private Key Password:	*****
Private Key Type:	2048-bit RSA
Digest Algorithm:	SHA-512
<b>Submit</b> <b>Cancel</b>	

3. Enter the information for each of the required parameters as described in [Table 37](#).

**Table 37: Parameters for Creating a Certificate Signing Request**

Parameter	Action/Description
Common Name	Displays the name associated with this entity. This can be a host name, IP address, or other name. The default is the fully-qualified domain name (FQDN). This field is mandatory.
Organization (O)	Specify the name of the organization. This field is optional.
Organizational Unit (OU)	Specify the name of the department, division, or section. This field is optional.
Location (L) State (ST) Country (C)	Specify the name of the state, country, and/or another location. These fields are optional
Subject Alternate Name (SAN)	Specify the alternative names for the specified Common Name. <b>NOTE:</b> Specify the SAN in the following formats: <ul style="list-style-type: none"><li>● email: <i>email_address</i></li><li>● URI: <i>url</i></li><li>● IP: <i>ip_address</i></li><li>● dns: <i>dns_name</i></li><li>● rid: <i>id</i></li></ul> This field is optional.
Private Key Password	1. Enter the private key password, then reenter it to verify the password.
Private Key Type	2. Select the length for the generated private key types from the following options: <ul style="list-style-type: none"><li>● 1024-bit RSA</li><li>● 2048-bit RSA</li><li>● 4096-bit RSA</li><li>● X9.62/SECG curve over a 256 bit prime field</li><li>● NIST/SECG curve over a 384 bit prime field</li></ul> The default private key type is <b>2048-bit RSA</b> .
Digest Algorithm	3. Select one of the following message digest algorithms: <ul style="list-style-type: none"><li>● MD5</li><li>● SHA-1</li><li>● SHA-224</li><li>● SHA-256</li><li>● SHA-384</li><li>● SHA-512</li></ul> <b>NOTE:</b> The MD5 algorithm is not available in FIPS mode.

4. When satisfied with the certificate signing request parameter settings, click **Submit**.

The **Create Certificate Signing Request** is generated and displayed (see [Figure 123](#)).

**Figure 123** *Displayed View of the Create Certificate Signing Request*



5. Copy the contents of the certificate request into a text file so that you can paste it into the Directory Certificate Services web form as described in [Obtaining a Signed Certificate from Active Directory on page 169](#).
6. To save the Certificate Signing Request file and the private key password file, click **Download CSR and Private Key Files**.



Be sure to note the location where you save the Certificate Signing Request and the private key password files.

## Importing the Root CA Files to the Certificate Trust List

Make sure the root Certificate Authority (CA) certificate and any intermediate CA certificates are downloaded as separate base-64-encoded files and imported into the Certificate Trust List in ClearPass *before* starting this operation.

To import the root CA files into the ClearPass server Certificate Trusted List:

1. Get the root CA certificate and any intermediate CA certificates from your Active Directory administrator. This typically consists of a root CA certificate and one or more intermediate CA certificates.
2. In ClearPass Policy Manager, navigate to **Administration > Certificates > Trust List**.

**Figure 124 Certificate Trust List**

#	Subject	Validity	Enabled
1.	C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA	valid	Disabled
2.	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Universal CA, CN=TC TrustCenter Universal CA I	valid	Disabled
3.	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High-Assurance Secure Server CA	valid	Disabled
4.	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	valid	Enabled
5.	CN=InCommon Server CA, OU=InCommon, O=Internet2, C=US	valid	Enabled
6.	<b>CN=ns-ISCA-CA, DC=ns, DC=arubatac, DC=us</b>	<b>valid</b>	<b>Enabled</b>
7.	CN=ns-RCA-CA, DC=ns, DC=arubatac, DC=us	valid	Enabled
8.	C=PL, O=Unizeto Sp. z o.o., CN=Certum CA	valid	Disabled
9.	C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root	valid	Enabled
10.	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	valid	Disabled

- To add the certificate file(s) to the Certificate Trust List, click **Add**, then browse to the root CA certificate file on your computer.

Be sure to add the root CA file first, then add the intermediate CA files after you've added the root CA file.



The root CA certificate file is now listed in the Certificate Trust List.

**Figure 125 New Root CA Files Added to the Certificate Trust List**

#	Subject	Validity	Enabled
1.	C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA	valid	Disabled
2.	C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Universal CA, CN=TC TrustCenter Universal CA I	valid	Disabled
3.	C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High-Assurance Secure Server CA	valid	Disabled
4.	CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	valid	Enabled
5.	CN=InCommon Server CA, OU=InCommon, O=Internet2, C=US	valid	Enabled
6.	<b>CN=ns-ISCA-CA, DC=ns, DC=arubatac, DC=us</b>	<b>valid</b>	<b>Enabled</b>
7.	<b>CN=ns-RCA-CA, DC=ns, DC=arubatac, DC=us</b>	<b>valid</b>	<b>Enabled</b>
8.	C=PL, O=Unizeto Sp. z o.o., CN=Certum CA	valid	Disabled
9.	C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root	valid	Enabled
10.	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	valid	Disabled

- Make sure the **Enabled** column for the newly added certificate says *Enabled*, which is the status displayed when you successfully import a certificate manually.
- Repeat steps 2, 3, and 4 for each certificate you received from your Active Directory administrator.

## Obtaining a Signed Certificate from Active Directory

This section describes how to obtain a signed server certificate from Active Directory.



Before you begin this operation, have the copy of the Certificate Signing Request at hand, as described in Step 4 of [Creating a Certificate Signing Request on page 165](#).

Also note the location where you saved the Certificate Signing Request and the private key password files, as you will need to retrieve these items to complete this operation.

To obtain a signed certificate from Active Directory:

1. Navigate to the **Microsoft Active Directory Certificate Services** page:

**Figure 126** Microsoft Active Directory Certificate Services Page

Microsoft Active Directory Certificate Services -- ns-ISCA-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#) Request a certificate

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

2. Click **Request a certificate**.

**Figure 127** Request a Certificate

Microsoft Active Directory Certificate Services -- ns-ISCA-CA

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

3. Choose **advanced certificate request**.

The **Submit a Certificate Request or Renewal Request** dialog opens.

This operation submits a saved certificate request to the Certificate Authority.

**Figure 128 Submit a Certificate Request**

The screenshot shows the 'Submit a Certificate Request or Renewal Request' page. At the top, there is a note: 'To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.' Below this is a 'Saved Request:' text area containing a base-64-encoded certificate request. A 'Certificate Template:' dropdown menu is set to 'User'. Under 'Additional Attributes:', there is a text area for 'Attributes:' which is currently empty. At the bottom right is a 'Submit >' button.

4. Copy the contents of the Certificate Signing Request into the **Saved Request** text box.
5. In the **Certificate Template** drop-down menu, select **Web Server**.

[Figure 129](#) shows an example of the completed Certificate Request web form.

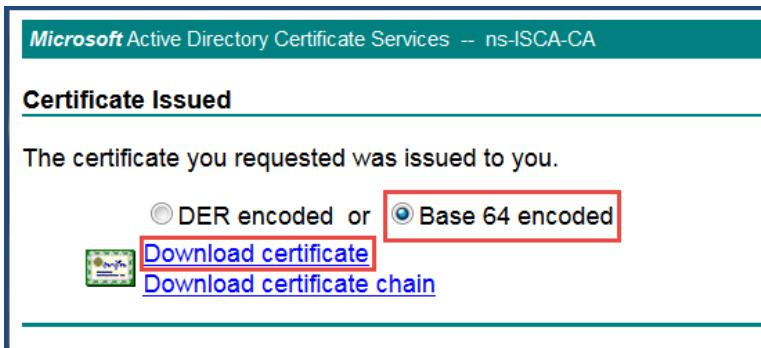
**Figure 129 Completed Submit a Certificate Request Dialog**

The screenshot shows the same 'Submit a Certificate Request or Renewal Request' page as Figure 128, but with the 'Saved Request:' text area populated with a large base-64-encoded certificate request. The 'Certificate Template:' dropdown menu is now set to 'Web Server'. The 'Additional Attributes:' text area is empty. At the bottom right is a 'Submit >' button.

6. Click **Submit**.

The **Certificate Issued** dialog opens.

**Figure 130** Certificate Issued



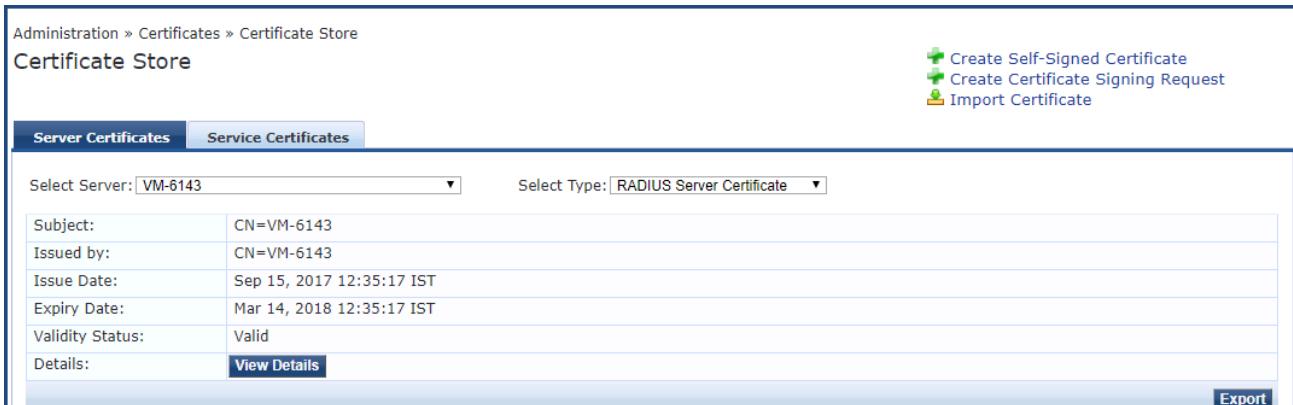
7. Do the following:
  - a. Select **Base 64 encoded**.  
Base-64 encoding is used for 802.1X authentication.
  - b. Click **Download certificate**.  
The server certificate is downloaded to your system.
  - c. Be sure to note the name of the downloaded certificate so that you can identify it when you import the server certificate into the ClearPass Policy Manager server.

## Importing a Server Certificate into ClearPass

To import a server certificate into ClearPass:

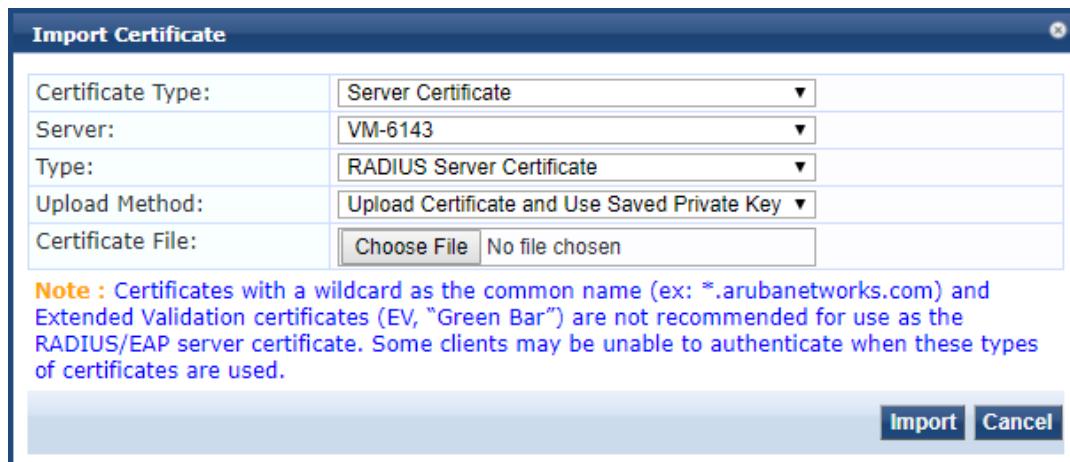
1. Navigate to **Administration > Certificates > Certificate Store**.  
The **Certificate Store** page opens.

**Figure 131** Certificate Store Page



2. From the **Server Certificates** tab, click the **Import Certificate** link.  
The **Import Certificate** dialog opens:

**Figure 132 Import Certificate Dialog**



 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 38: Import Server Certificate Parameters**

Parameter	Action/Description
Certificate Type	<b>Server Certificate</b> is selected by default.
Server	Displays the name of the selected ClearPass server.
Type	Displays the type of server certificate that was selected: <ul style="list-style-type: none"><li>● RADIUS Server Certificate</li><li>● HTTPS Service Certificate</li></ul>

Parameter	Action/Description
Upload Method	<p>Select one of the following methods to upload the certificate:</p> <ul style="list-style-type: none"> <li>● <b>Upload Certificate and Use Saved Private Key</b> This option allows the administrator to upload only the certificate. The certificate is then matched against the private key saved on the ClearPass server.</li> <li>● <b>Upload PKCS#12 Certificate (.pfx or .p12 only)</b> With this option, the administrator uploads the PKCS#12 file and provides a pass phrase.</li> <li>● <b>Upload Certificate and Private Key Files</b> The administrator can choose to upload the private key file and password along with the certificate file.</li> </ul>
Certificate File	<p>Browse to the certificate file to be imported.</p> <p><b>NOTE:</b> Both certificates with a wild card 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.</p>

4. Click **Import**.

The selected server certificate is imported into ClearPass. The Server Certificate screen displays the message:

*Server Certificate updated successfully. Please log in again to continue.*

5. Log out of the ClearPass server, then log in again to resume operations on this server.

## Manually Testing Login Credentials Against Active Directory

To test a username and password against the Active Directory, run the **ad auth** command in the Policy Manager CLI.

This command manually checks against Active Directory to indicate whether or not a username and password are valid.

1. Enter the following CLI command:

```
(server) # ad auth -u <username> -n <NetBIOS_domain_name>
■ -u indicates the username.
■ -n indicates the NetBIOS domain name.
```

For example:

```
(server) # ad auth -u administrator -n COLLEGE
```

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.

# Preparing for 802.1X Wireless Authentication with Active Directory

This chapter includes the following information:

- [About 802.1X Authentication](#)
- [What Is AAA?](#)
- [Walking Through an 802.1X Authentication Scenario](#)
- [Configuring 802.1X Wireless Authentication with Active Directory](#)
- [Troubleshooting 802.1X Configuration Issues](#)

## About 802.1X Authentication

This section contains the following information:

- [Introducing 802.1X](#)
- [802.1X Authentication Components](#)

### Introducing 802.1X

This chapter describes how to configure 802.1X wireless authentication with Active Directory® in an Aruba network.

802.1X is an IEEE standard and a method for authenticating the identity of a user before providing network access to the user. 802.1X provides an authentication mechanism to devices that need to attach to a wireless LAN or a wired LAN.

RADIUS (Remote Authentication Dial In User Service) is a protocol that provides centralized authentication, authorization, and accounting management (for details, see [What Is AAA? on page 176](#)).

For authentication purpose, the wireless client can associate with a network access server (NAS) or a RADIUS client. ClearPass is a RADIUS server. The wireless client can pass data traffic only after successful 802.1X authentication.

- 802.1X offers the capability to permit or deny network connectivity based on the identity of the end user or device.
- 802.1X enables port-based access control using authentication. An 802.1X-enabled port can be dynamically enabled or disabled based on the identity of the user or device that connects to it.

Before authentication, the identity of the endpoint is unknown and all traffic is blocked. After authentication, the identity of the endpoint is known and all traffic from that endpoint is allowed.

### 802.1X Authentication Components

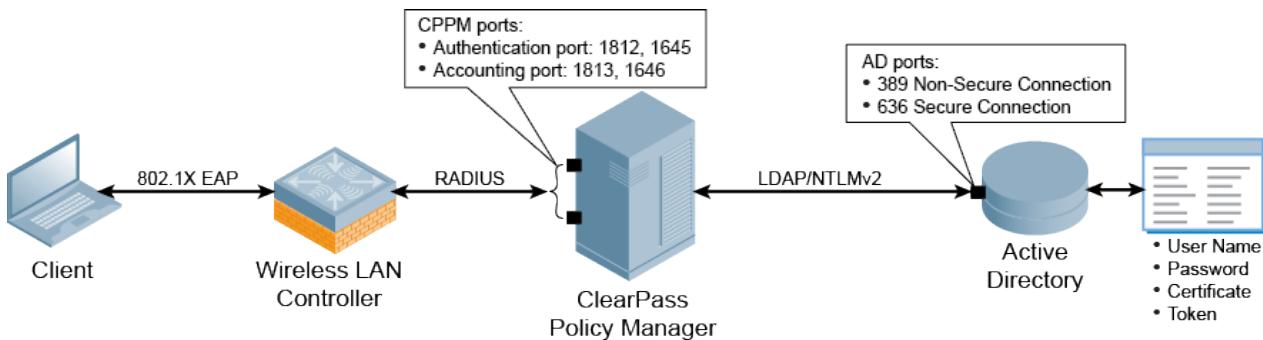
802.1x authentication consists of three components—a *supplicant*, an *authenticator*, and an *authentication server* (see [Figure 133](#)).

- The *supplicant*, or client, is the device attempting to gain access to the network. You can configure the user-centric network to support 802.1x authentication for wired users as well as wireless users.
- The *authenticator* is the gatekeeper to the network and permits or denies access to the supplicants. The mobility controller acts as the authenticator, relaying information between the authentication/ClearPass server and the supplicant. The EAP type must be consistent between the

authentication server and supplicant and is transparent to the mobility controller.

- The *authentication server* is typically a host running software supporting the RADIUS and EAP protocols. It provides a database of information required for authentication and informs the authenticator to deny or permit access to the supplicant. In this guide, the authentication server is the ClearPass Policy Manager server.

**Figure 133** 802.1X Authentication Network Components



[Table 39](#) describes each of the ClearPass firewall ports that are used by Active Directory.

**Table 39: Active Directory ClearPass Firewall Ports**

Firewall Port	Description
UDP Port 88	Used for Kerberos authentication.
TCP and UDP Port 135	Used for domain controller-to-domain controller and client-to-domain controller operations.
UDP Port 389	Used for LDAP to handle normal queries from client computers to the domain controllers.
TCP and UDP Port 445	Used for Kerberos password change.
TCP Ports 3268 and 3269	Used for Global Catalog distribution from the client to the domain controller. The Global Catalog makes the directory structure within a forest transparent to users who perform a search. In a multidomain Active Directory Domain Services forest, the Global Catalog provides a central repository of domain information for the forest by storing partial replicas of all domain directory partitions. These partial replicas are distributed by multimaster replication to all Global Catalog servers in a forest.
TCP and UDP Port 53	Used for DNS from the client to the domain controller and from the domain controller to another domain controller.
ICMP types echo (8) and echo-reply (0)	The Internet Control Message Protocol (ICMP) has many messages that are identified by a <b>Type</b> field. ICMP types <b>echo (8)</b> and <b>echo-reply (0)</b> are used between the ClearPass host and the domain controller during the domain join operation (see <a href="#">Joining a ClearPass Server to an Active Directory Domain on page 144</a> ).

## What Is AAA?

AAA stands for *authentication*, *authorization*, and *accounting*.

AAA is a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These processes working in concert are important for effective network management and security.

### Authentication

Authentication provides a method of identifying a user, typically by having the user enter a valid username and password before access to the network is granted. Authentication is based on each user having a unique set of login credentials for gaining network access.

The AAA server compares a user's authentication credentials with other user credentials stored in a database; in this case, that database is Active Directory. If the user's login credentials match, the user is granted access to the network. If the credentials don't match, authentication fails and network access is denied.

### Authorization

Following authentication, a user must gain authorization for doing certain tasks. After logging in to a system, for instance, the user may try to issue commands. The authorization process determines whether the user has the authority to issue such commands.

Simply put, authorization is the process of enforcing policies—determining what types or qualities of activities, resources, or services a user is permitted. Usually authorization occurs within the context of authentication. After you have authenticated a user, they may be authorized for different types of access or activity.

As it relates to network authentication via RADIUS and 802.1x, authorization can be used to determine what VLAN, Access Control List (ACL), or user role that the user belongs to.

### Accounting

The final piece in the AAA framework is accounting, which monitors the resources a user consumes during network access. This can include the amount of system time or the amount of data sent and received during a session.

Accounting is carried out by logging session statistics and usage information. It is used for authorization control, billing, trend analysis, resource utilization, and planning for the data capacity required for business operations.

ClearPass Policy Manager functions as the accounting server and receives accounting information about the user from the Network Access Server (NAS). The NAS must be configured to use ClearPass Policy Manager as an accounting server, and it is up to the NAS to provide accurate accounting information to ClearPass Policy Manager.

## Configuring 802.1X Wireless Authentication with Active Directory

This section contains the following information:

- [Authenticating Against Active Directory](#)
- [About the 802.1X Wireless Service](#)
- [Creating the 802.1X Wireless Service](#)
- [Deleting a ClearPass Policy Manager Service](#)

This section describes how to use the ClearPass Policy Manager to configure 802.1X authentication with Active Directory in an Aruba network.

## Authenticating Against Active Directory

802.1x authentication can be used to authenticate users or computers against a user database or domain such as Microsoft Active Directory (for related information, see [Preparing for Active Directory Authentication on page 144](#)).

The supplicant (wireless client) authenticates against the RADIUS server (which is the authentication server/ClearPass Policy Manager server) using an EAP method configured on both the supplicant and the RADIUS server. They will, in turn, negotiate which EAP method to use based on the list of EAP methods each one supports.

The mobility controller's (authenticator) role is to send authentication messages between the supplicant and authentication server. This means the RADIUS server is responsible for authenticating users.)

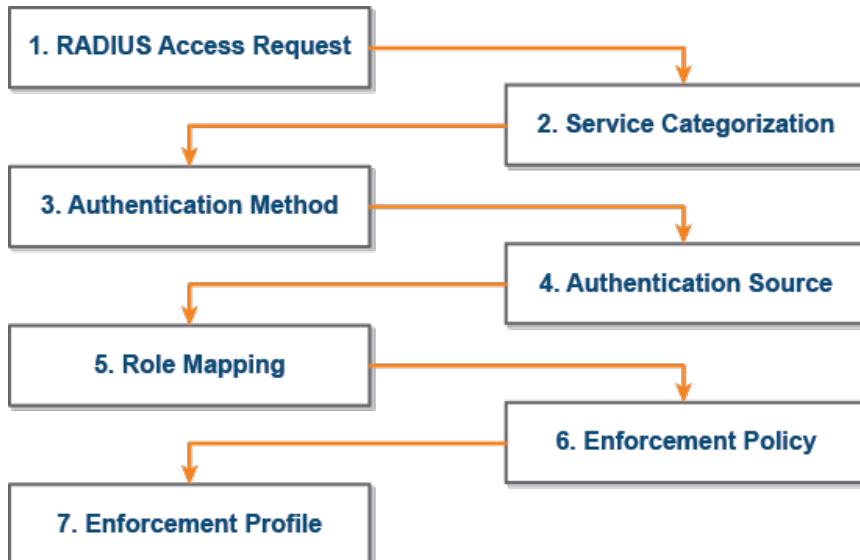
Mobility controllers perform EAP exchanges between the supplicant and convert these to RADIUS access-request messages that are sent to the RADIUS server's IP address and the specified UDP port (for details, see [802.1X EAP-PEAP Reference on page 276](#)).

## About the 802.1X Wireless Service

The basic Policy Manager use case configures a Policy Manager Service to identify and evaluate a RADIUS request from a user logging into a Mobility Controller.

[Figure 134](#) illustrates the authentication process flow for an 802.1X Wireless Service.

**Figure 134** 802.1X Wireless Service Authentication Process Flow



[Table 40](#) provides descriptions of each of the 802.1X authentication processes illustrated in [Figure 134](#).

**Table 40:** Description of the 802.1X Authentication Processes

	<b>Authentication Process</b>	<b>Description</b>
1	RADIUS Access-Request	The Network Access Server (NAS) sends a RADIUS access request to Policy Manager, which then evaluates the request and identifies RADIUS connection control attributes.
2	Service Categorization	Based on the RADIUS connection control attributes identified by Policy Manager, the request will be categorized into a Policy Manager service.
3	Authentication Method	Policy Manager attempts to authenticate the user (in order of priority) using the authentication method defined in the Policy Manager service.
4	Authentication Source	After negotiating an authentication method with the user, Policy Manager authenticates the user (in order of priority) against the authentication sources defined in the Policy Manager service.
5	Role Mapping	Any roles defined in role-mapping policies or automatically assigned by Policy Manager based on several sources of information, including RADIUS connection control attributes, authentication sources, or authorization attributes.
6	Enforcement Policy	An enforcement policy is a way to organize enforcement profiles and apply them to users or Policy Manager roles. Based on the enforcement policy assigned to the role, enforcement profiles are applied to the service request.
7	Enforcement Profile	Enforcement profiles are the building blocks that control network access and define types of access. Multiple enforcement profiles can be used in an enforcement policy.

For a detailed description of the EAP-PEAP-MSCHAPV2 process, refer to [A Tour of the EAP-PEAP-MSCHAPv2 Ladder on page 276](#).

## Creating the 802.1X Wireless Service

The 802.1X Wireless Service provides a method for wireless end-hosts connecting through an 802.1X wireless access device or mobility controller, with authentication using IEEE 802.1X and with service rules customized for Mobility Controllers.

This ClearPass 802.1X template guides you through the following tasks:

- Selecting an Active Directory Authentication Source.  
This guide assumes that the Active Directory Authentication Source has already been configured. For details, see [Preparing for Active Directory Authentication on page 144](#).
- Selecting a Mobility Controller.  
This guide assumes that the mobility controller to be used for 802.1X authentication has already been configured. For details, see [Preparing the Mobility Controller for ClearPass Policy Manager Integration on page 34](#).
- Creating an Enforcement Policy for Active Directory-based attributes.

The procedure for creating an Enforcement Policy is described in this section.

To create an 802.1X wireless service:

- From ClearPass Policy Manager, navigate to **Configuration > Start Here > Aruba 802.1x Wireless**.  
The **General** page for the ClearPass 802.1X Wireless Service template opens.

**Figure 135** General Page in the 802.1X Wireless Service Template

Configuration > Start Here  
Service Templates - Aruba 802.1X Wireless

**General**   **Authentication**   **Wireless Network Settings**   **Posture Settings**   **Enforcement Details**

Name Prefix\*:

Description  
For wireless end-hosts connecting through an Aruba 802.11 wireless access device or controller, with authentication via IEEE 802.1X (Service rules customized for Aruba WLAN Mobility Controllers). This template configures an AD Authentication Source; joins this node to the AD Domain; creates Enforcement Policy for AD based attributes; and creates an Aruba Network Access Device.

[Back to Start Here](#)   [Delete](#)   [Next >](#)   [Add Service](#)   [Cancel](#)

- In the *Name Prefix* field, enter a prefix that is appended to services using this template, then click **Next**.  
The **Authentication** page opens.
- From the **Select Authentication Source** drop-down list, select the name of the Active Directory, as shown in [Figure 136](#), then click **Next**.

**Figure 136** Selecting the Active Directory

ClearPass Policy Manager   [Support](#) | [Help](#) | [Logout](#)  
admin (Super Administrator)

Configuration > Start Here  
Service Templates - Aruba 802.1X Wireless

**General**   **Authentication**   **Wireless Network Settings**   **Posture Settings**   **Enforcement Details**

Select Authentication Source: ✓ Create a new Active Directory  
College AD

Create an Active Directory

Active Directory Name\*:

Description:

Server\*:

Port\*: 389 (For secure connection, use port 636)

Identity\*:  (e.g., administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)

Password\*:

NETBIOS\*:

Base DN\*:  (e.g., CN=Users,DC=example,DC=example,DC=com)

[Back to Start Here](#)   [Delete](#)   [Next >](#)   [Add Service](#)   [Cancel](#)

When you choose an existing Authentication Source, the information in the **Authentication** and **Enforcement Details** pages is populated automatically.

The **Wireless Network Settings** page opens.

- Select the mobility controller you defined earlier (for details, see [Preparing the Mobility Controller for ClearPass Policy Manager Integration on page 34](#)).

**Figure 137** Selecting the Mobility Controller

The fields in the **Wireless Network Settings** page are automatically populated with the selected mobility controller's configuration information.

5. Click **Next**.

The **Posture Settings** page opens.

**Figure 138** Enabling Posture Checks

ClearPass Policy Manager performs automated endpoint health checks and posture assessments to ensure that devices are compliant before they connect to mobile networks.

6. To enable posture checks to be performed after the authentication process completes, click the **Enable Posture Checks** check box, then click **Next**.

The **Enforcement Details** page opens.

Figure 139 shows an example of a new Enforcement Policy, with three attributes defined:

- If **memberOf** equals **Faculty**, then assign Role **Faculty**.
- If **memberOf** equals **Students**, then assign Role **Students**.
- If **memberOf** equals **Contractors**, then assign Role **Contractors**.

**Figure 139** Creating a New Enforcement Policy

The screenshot shows the 'ClearPass Policy Manager' interface with the title 'Service Templates - Aruba 802.1X Wireless'. The 'Enforcement Details' tab is selected. A table titled 'Create a new Enforcement Policy' lists rules for assigning Aruba roles based on user attributes. The rules defined are:

Attribute Name	Attribute Value	Aruba Role
If [Department]	equals Engineering	then assign Role authenticated
If [Name]	equals JMcCoy	then assign Role Contractor
If [Account Expires]	equals	then assign Role
Default Role*:		Employee
Initial Role*:		initial
Quarantine Role*:		quarantine

Buttons at the bottom include 'Back to Start Here', 'Delete', 'Next >', 'Add Service', and 'Cancel'.

**Table 41:** Enforcement Policy Configuration Settings

Parameter	Action/Description
Attribute Name	<p>The attributes defined in the Authentication Source are listed here.</p> <ol style="list-style-type: none"> <li>Configure an optional enforcement policy based on the following attributes: <ul style="list-style-type: none"> <li>Department</li> <li>Email</li> <li>Name</li> <li>Phone</li> <li>Title</li> <li>UserDN</li> <li>company</li> <li>member of</li> </ul> </li> </ol>
Attribute Value	<ol style="list-style-type: none"> <li>Enter the Active Directory attribute value for the selected name in the <i>Attribute Name</i> field.</li> </ol>
Aruba Role	<ol style="list-style-type: none"> <li>Assign a user role to the Enforcement Policy. The configured user roles are defined in the mobility controllerspecified for this service.</li> </ol> <p>To see the list of configured user roles defined in the mobility controller:</p> <ol style="list-style-type: none"> <li>Log in to the Mobility Controller.</li> <li>Navigate to <b>Configuration &gt; SECURITY &gt; Access Control</b>. The User Roles page is displayed.</li> </ol>

This completes the base configuration for a new 802.1X Wireless Service.

4. Click **Add Service**.

An entry for the new set of configurations is created under the Services, Roles, Role Mapping, Enforcement Policies, and Profiles menus.

A summary for the 802.X service you configured is displayed.

**Figure 140** Summary of the 802.1X Service Configuration

The screenshot shows the 'Services' configuration page. At the top right, there are three buttons: 'Add' (green plus), 'Import' (yellow arrow), and 'Export All' (blue arrow). Below these, a message box displays:

- Added 5 Enforcement Profile(s)
- Added 1 Enforcement Policies
- Added 1 service(s)

Below the message box is a search bar with 'Filter: Name' and a dropdown menu. To the right of the search bar are 'Go' and 'Clear Filter' buttons. Further right are 'Show 10 records' and a 'Reorder' button.

#	Order ▲	Name	Type	Template	Status
1.	<input type="checkbox"/>	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	<span style="color: green;">●</span>
2.	<input type="checkbox"/>	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement ( Generic )	<span style="color: green;">●</span>
3.	<input type="checkbox"/>	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	<span style="color: green;">●</span>
4.	<input type="checkbox"/>	[Guest Operator Logins]	Application	Aruba Application Authentication	<span style="color: green;">●</span>
5.	<input checked="" type="checkbox"/>	College AD Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	<span style="color: green;">●</span>

At the bottom left of the table area, it says 'Showing 1-5 of 5'. At the bottom right are 'Copy', 'Export', and 'Delete' buttons.

## Deleting a ClearPass Policy Manager Service

You can only delete ClearPass services that have been created by an administrator. Default services cannot be deleted.

To delete a ClearPass Policy Manager service:

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

The **Configuration > Services** page opens.

**Figure 141** Deleting a ClearPass Service

The screenshot shows the 'Services' configuration page. At the top right, there are three buttons: 'Add' (green plus), 'Import' (yellow arrow), and 'Export All' (blue arrow). Below these, the user is identified as 'admin (Super Administrator)'.

#	Order ▲	Name	Type	Template	Status
1.	<input type="checkbox"/>	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	<span style="color: green;">●</span>
2.	<input type="checkbox"/>	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement ( Generic )	<span style="color: green;">●</span>
3.	<input type="checkbox"/>	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	<span style="color: green;">●</span>
4.	<input checked="" type="checkbox"/>	[Guest Operator Logins]	Application	Aruba Application Authentication	<span style="color: green;">●</span>

At the bottom left of the table area, it says 'Showing 1-4 of 4'. At the bottom right are 'Reorder', 'Copy', 'Export', and 'Delete' buttons.

2. Select the appropriate service's check box, then click **Delete**.

All the configured entries under the Services, Authentication Source, Roles, Role Mapping, Enforcement Policies, and Profiles menus are deleted (if these entities were created from the Service Template).



Do not delete entities used in service configurations that were not created using the Service Template.

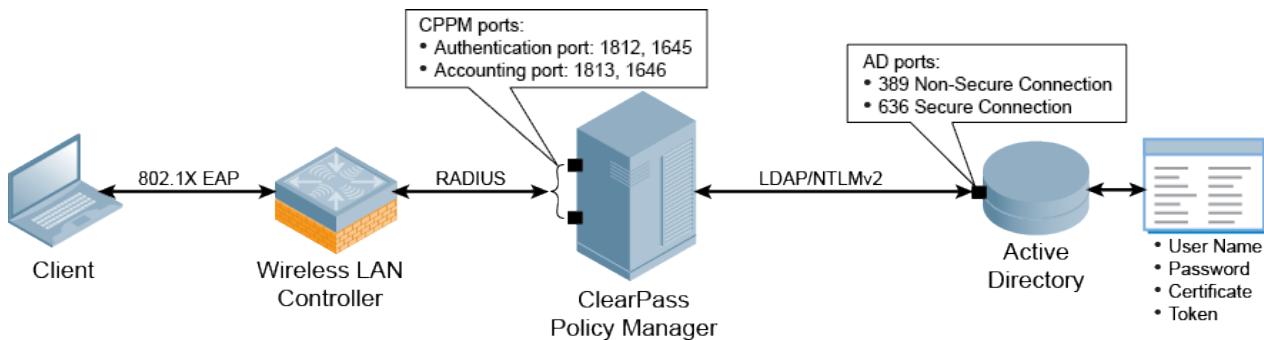
## Walking Through an 802.1X Authentication Scenario

This section shows the flow of traffic for 802.1X authentication traffic for wireless and wired authentication scenarios and provides a typical example of the 802.1X authentication process.

### 802.1X Wireless Authentication Traffic Flow

[Figure 142](#) shows the flow of traffic for 802.1X authentication using Active Directory.

**Figure 142** Traffic Flow for 802.1X Wireless Authentication with Active Directory



### Walking Through the 802.1X Authentication Process

Let's use an example to walk through the authentication process as illustrated in [Figure 142](#).

1. A Sales Dept. employee connects to the Aruba wireless network from her laptop and an 802.1X EAP-PEAP authentication process begins automatically.  
EAP-PEAP (Protected Extensible Authentication Protocol) is the protocol used to communicate between the client and the network device, in this case, a mobility controller. For details, see .
2. The client's authentication request is sent to the mobility controller.
3. When the mobility controller receives the authentication request, it sends a RADIUS access-request packet to the ClearPass Policy Manager server with the encrypted user name and password.  
RADIUS is the protocol that network access device (NAD) authenticators use to communicate with the ClearPass server in order to look up the information in the RADIUS database, which in this example is Active Directory.
4. The ClearPass Policy Manager server checks the Active Directory database for a matching user name and password.

The communication between the ClearPass Policy Manager server and Active Directory is via NT LAN Manager (NTLM) for authentication in conjunction with Lightweight Directory Access Protocol (LDAP) for search and directory lookup.

- If there is not a match, the ClearPass server sends an *access-reject* message to the mobility controller and the Sales Dept. employee is denied access to the network.
- If there is a match, the ClearPass server sends an *access-accept* message to the mobility controller, and the Sales Dept. employee is granted access to the network.

### User Role Attribute Information

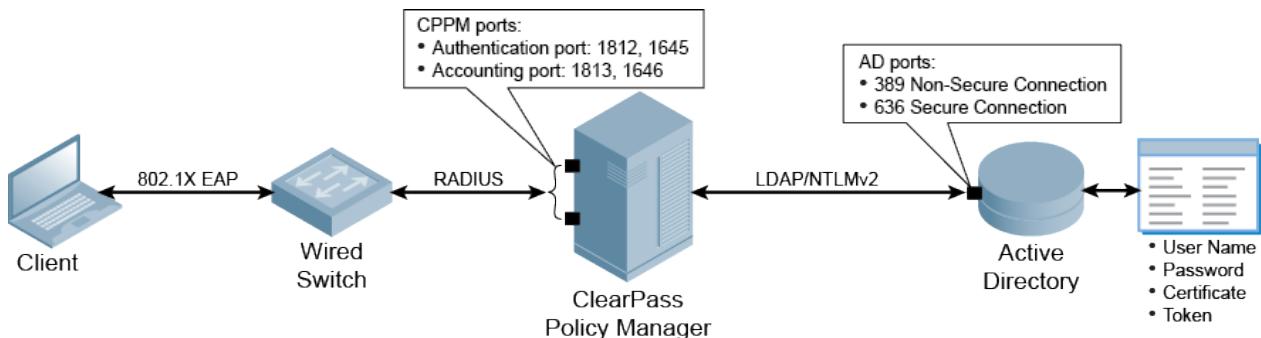
The ClearPass Policy Manager server can also send attribute information about the user (for example, User Role) to the mobility controller. In this example, the server uses the User Role attribute, which indicates that the user is in the Sales Department.

The mobility controller applies a Sales Department firewall role to this user's traffic. Typically for such a role, the firewall rule applied would be *IP any permit*, which permits all IP traffic.

## 802.1X Wired Authentication Traffic Flow

This same process applies to wired clients that connect to an ArubaOS switch or a third-party switch and perform 802.1X authentication to the ClearPass Policy Manager server (see [Figure 143](#)).

**Figure 143** *Traffic Flow for 802.1X Wired Authentication with Active Directory*



For more information about the Aruba ArubaOS Switch and 802.1X authentication, see [Integrating the ArubaOS Switch with ClearPass on page 186](#).

## Troubleshooting 802.1X Configuration Issues

This section provides information on troubleshooting potential trouble spots when configuring Active Directory and the Mobility Controller.

### Active Directory Authentication Source Configuration Issues

1. If you have configured a host name instead of an IP address for the Active Directory server in the **Primary** tab > **Hostname** field, ensure that the Active Directory hostname is resolved to an IP address by the Domain Name System (DNS).
2. Ensure the Bind DN credentials have read access to the Active Directory locations where users and computers are present.
3. Verify that the user name used for Bind DN is not locked in the Active Directory.
4. While joining ClearPass to the Active Directory domain, use the *Fully Qualified Domain Name* (FQDN) of the Active Directory host and not just the Domain Name.
5. Verify that the ClearPass server's time is synchronized with the Active Directory, as a clock skew will cause the join domain operation to fail (for details, see [Confirming NTP Server Synchronization on page 146](#)).

 The maximum allowed clock skew between the ClearPass server and the Active Directory server is five minutes.

### Mobility Controller Configuration Issues

1. Ensure that the Role information that was sent to the mobility controller via enforcement matches the role defined in the mobility controller.
2. If authentication requests are not visible in the Access Tracker (**Monitoring > Live Monitoring > Access Tracker**), verify the following:

- a. Verify the shared secret in the mobility controller and ClearPass Policy Manager's Network Access Device configuration. Shared secret errors are shown in the ClearPass Policy Manager Event Viewer (**Monitoring > Event Viewer**).
- b. Ensure that the mobility controller's IP address is configured correctly in ClearPass Policy Manager.  
Any mismatch will show ERROR/WARN events in the Event Viewer stating that an authentication request is received from an unknown IP address.

This chapter describes the process of integrating ArubaOS switches with ClearPass. This chapter includes the following information:

- [About the ArubaOS Switch](#)
- [Initial ArubaOS Switch Configuration](#)
- [Setting Up RADIUS Authentication, Authorization, and Accounting](#)
- [Authenticating Users to the ArubaOS Switch](#)
- [Switch Management Using TACACS+](#)
- [Switch Management Using RADIUS](#)
- [Monitoring and Troubleshooting](#)

## About the ArubaOS Switch

This section contains the following information:

- [Overview](#)
- [Unified Management with ClearPass Policy Manager](#)

### Overview

The ArubaOS Switch Series is a mobile campus-access solution for enterprises, small- and medium-size businesses, and branch-office networks.

The ArubaOS Switch provides the following high-level features:

- HPE Smart Rate ports support multi-Gigabit Ethernet speeds (1, 2.5, 5, and 10 Gigabit Ethernet) for high speed 802.11ac devices on existing cabling for cost-effective and convenient network upgrades with no rip and replacement of cabling required.
- Delivers a consistent wired and wireless user experience by supporting unified management tools such as ClearPass Policy Manager and Aruba AirWave.
- Provides optimal configuration automatically when connected to Aruba Access Points (APs) for Power-over-Ethernet (PoE) priority, VLAN configuration, and rogue AP containment.
- Right-sizes deployment and back-haul capacity with modular 10 GbE and 40 GbE uplinks. Full PoE+ provisioning on all switch ports. Dual, redundant, hot-swappable power supplies and innovative backplane stacking technology delivers resiliency and scalability in a convenient 1U form factor.
- Advanced Layer-2 and Layer-3 feature set with OSPF, IPv6, IPv4 BGP, robust QoS and policy-based routing are included with no software licensing required. With support for OpenFlow, the ArubaOS switch takes advantage of SDN applications such as HPE Network Visualizer, Optimizer, and Protector Applications.
- For a better mobile-first campus experience, the ArubaOS switch provides powerful Aruba Layer-3 switch series with backplane stacking, low latency, resiliency, and OpenFlow.

## Unified Management with ClearPass Policy Manager

The ArubaOS Switch Series supports Aruba ClearPass Policy Manager to provide unified and consistent policy between wired and wireless users. The switch includes simplified implementation and management of guest login, user onboarding, network access, security, QoS, and other network policies on the network.

- Supports Aruba AirWave to provide a common platform for zero-touch provisioning, management, and monitoring for wired and wireless network devices.
- RMON, XRMON, and sFlow provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events.
- The out-of-band Ethernet management port (eth0) keeps management traffic segmented from your network data traffic.

## Initial ArubaOS Switch Configuration

This section describes the tasks required for initial ArubaOS switch configuration. This section contains the following information:

- [Configuring Administrator Credentials](#)
- [Configuring the IP Address of the Out-of-Band Management Port](#)
- [Configuring SNMPv3](#)
- [Configuring a ClearPass/RADIUS Server on the Switch](#)
- [Defining the ArubaOS Switch in ClearPass](#)

### Configuring Administrator Credentials

The first task in the initial setup for the ArubaOS switch is to configure the administrator credentials.

To configure the ArubaOS switch administrator credentials:

1. Enter configuration mode.

```
ArubaOS-switch# configure
```

2. Create a local administrative account to be used when RADIUS or TACACS+ authentication is unavailable.

```
ArubaOS-switch(config)# password manager user-name ladmin
```

### Configuring the IP Address of the Out-of-Band Management Port



This procedure assumes that switch management will be done using out-of-band management.

To configure the ArubaOS switch IP address of the out-of-band management port:

1. Enable out-of-band management (oobm).

```
ArubaOS-switch(config)# oobm enable
```

2. Assign an IP address to the oobm port.

```
ArubaOS-switch(config)# oobm ip address 10.2.100.68 255.255.255.0
```

3. Add a default gateway to the oobm port.

```
ArubaOS-switch(config)# oobm ip default-gateway 10.2.100.1
```

4. Save the configuration

```
ArubaOS-switch(config)# save
```

## Configuring SNMPv3

Aruba recommends using SNMPv3. SNMPv3 access requires an IP address and subnet mask configured on the switch. If you are using DHCP/Bootp to configure the switch, ensure that the DHCP/Bootp process provides the IP address.

- You can (optionally) restrict access to SNMPv3 agents only by using the **snmpv3 only** command.
- To restrict write-access to only SNMPv3 agents, use the **snmpv3 restricted-access** command.

### Adding a New User When SNMPv3 Is Already Configured

If SNMPv3 has already been configured on this switch, then the only task required is to add an SNMP v3 user.

To add a new user to an ArubaOS switch that already has SNMPv3 configured, issue the following command:

```
ArubaOS-switch (config)# snmpv3 user <user_name> auth sha <authentication_password> priv aes <privacy_password>
```

### Configuring SNMPv3 for the First Time

When you enable SNMPv3 operation on the switch, an initial user entry is generated with the authentication protocol set to **MD5** and the privacy protocol set to **DES** (Data Encryption Standard). This section describes how to change the privacy protocol from default setting of **DES** to the more secure protocol **AES** (Advanced Encryption Standard). This includes the creation of the initial user record.

When SNMPv3 is enabled, the ArubaOS switch begins the initialization process by creating an account named "initial."

To configure SNMPv3 for the first time on the ArubaOS switch:

1. ArubaOS-switch (config)# **snmpv3 enable**  
SNMPv3 Initialization process.  
Creating user 'initial'  
Authentication Protocol: MD5
2. Enter authentication password: \*\*\*\*\*  
Privacy protocol is DES.
3. Enter privacy password: \*\*\*\*\*  
User 'initial' has been created.
4. Would you like to create a user that uses SHA? [y/n] **y**
5. Enter user name: <*user\_name*>  
Authentication Protocol: SHA
6. Enter authentication password: \*\*\*\*\*  
Privacy protocol is DES.
7. Enter privacy password: \*\*\*\*\*  
User creation is done. SNMPv3 is now functional.
8. Would you like to restrict SNMPv1 and SNMPv2c messages to have read-only access (you can set this later by the command '**snmpv3 restricted-access**')? [y/n] **n**

 Restricting access to only SNMPv3 messages makes the community named "public" inaccessible to network management applications (such as autodiscovery, traffic monitoring, SNMP trap generation, and threshold setting) from operating in the ArubaOS switch. For that reason, Aruba recommends answering **no** to Step 8.

## Changing the Privacy Protocol to Secure Protocol AES

After enabling SNMPv3 for the first time, the user that is created during this process (in our example, **cp-snmp**) has the privacy protocol set to **DES**.

Because **AES** (Advanced Encryption Standard) is more secure, Aruba recommends changing the privacy protocol to **AES**.

To change the privacy protocol to **AES**, issue the following command:

```
ArubaOS-switch (config) # snmpv3 user <user_name> auth sha <authentication_password> priv aes <privacy_password>
```

## Configuring a ClearPass/RADIUS Server on the Switch

Before you begin this procedure, have at hand the following information:

- IP address of the target ClearPass server(s)
- RADIUS Shared Secret configured for the ClearPass server(s)

To configure a ClearPass/RADIUS server on the ArubaOS switch (also referred to as the Network Access Device (NAD)):

1. Log in to the ArubaOS switch via the console port or via SSH.
2. To add a ClearPass server node, enter the following commands:

```
ArubaOS-switch # config t
ArubaOS-switch(config) # radius-server host <ClearPass_IP_address> key <RADIUS_shared_secret>
ArubaOS-switch(config) # radius-server host <ClearPass_IP_address> dyn-authorization
ArubaOS-switch(config) # aaa server-group radius <GroupName> host <ClearPass_IP_address>
```

3. Repeat these commands to add additional ClearPass/RADIUS servers.
4. To view the current status of the ClearPass/RADIUS server configuration:

```
ArubaOS-switch(config) # show radius
```

**Figure 144** *show radius Command Output*

Status and Counters - General RADIUS Information					
Deadtime (minutes)	:	0			
Timeout (seconds)	:	5			
Retransmit Attempts	:	3			
Global Encryption Key	:				
Dynamic Authorization UDP Port	:	3799			
Source IP Selection	:	Outgoing Interface			
Server IP Addr	Auth Port	Acct Port	DM/CoA	Time Window	Encryption Key
10.	1812	1813	Yes	300	OOBM
10.	1812	1813	Yes	300	No

As shown in [Figure 144](#), running a **show radius** command displays the following information:

- The switch is listening for inbound CoA commands on the default UDP port of **3799**.
- Three ClearPass nodes have been defined to this switch.
- Authentication and Accounting are running on their default UDP ports **1812** and **1813**.

## Defining the ArubaOS Switch in ClearPass

To define the Network Access Device (NAD)—that is, the ArubaOS switch—in ClearPass:

1. In ClearPass, navigate to **Configuration > Network > Devices**.  
The **Network Devices** page opens.
2. Click the **Add** link.  
The **Add Device** dialog opens.

**Figure 145** Adding the ArubaOS Switch to ClearPass

The screenshot shows the 'Add Device' dialog box with the title 'Add Device'. It has tabs for Device, SNMP Read Settings, SNMP Write Settings, CLI Settings, OnConnect Enforcement, and Attributes. The Device tab is selected. The fields are as follows:

Name:	Aruba 3810M		
IP or Subnet Address:	10. [redacted] (e.g., 192.168.1.10 or 192.168.1.1/24 or 192.168.1.1-20)		
Description:	Aruba 3810M Switch		
RADIUS Shared Secret:	[redacted]	Verify:	[redacted]
TACACS+ Shared Secret:	[redacted]	Verify:	[redacted]
Vendor Name:	vlett-Packard-Enterprise		
Enable RADIUS CoA:	<input checked="" type="checkbox"/>	RADIUS CoA Port:	3799

At the bottom right are 'Add' and 'Cancel' buttons.

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

**Table 42:** Add Device Parameters for an ArubaOS Switch

Parameter	Action/Description
Name	Enter a descriptive name to identify the network device being added.
IP or Subnet Address	<ul style="list-style-type: none"><li>If this is a single device, enter its <b>IP address</b>.</li><li>If there are multiple devices in the same subnet that are being defined, enter the <b>subnet address</b>.</li></ul>
Description	Provide a more detailed set of information describing the network device (recommended).
RADIUS Shared Secret	Enter the password that will be used on both the ClearPass server and on the network device(s) to authenticate each other.
TACACS Shared Secret	If TACACS+ will be used on this device, enter the password that will be used on both the ClearPass server and on the network device(s) to authenticate each other.

Parameter	Action/Description
Vendor Name	For ArubaOS switches, choose <b>Hewlett-Packard-Enterprise</b> as the vendor name.
Enable RADIUS CoA	Make sure this check box is enabled. This parameter is enabled by default.
RADIUS CoA Port	If RADIUS CoA is enabled, this specifies the default port as <b>3799</b> . Change this value only if you defined a custom port. For related information, see <a href="#">Configuring ClearPass as an RFC 3576 (CoA) Server</a> .

## Setting Up RADIUS Authentication, Authorization, and Accounting

This section contains the following information:

- [About AAA Services](#)
- [About the RADIUS Protocol](#)
- [About the TACACS+ Protocol](#)
- [About RADIUS Authentication and Authorization](#)
- [Setting Up RADIUS Accounting](#)

### About AAA Services

AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers.

- *Authentication* identifies a user.
- *Authorization* determines what that user can do on the network.
- *Accounting* monitors the network usage time for billing purposes.

AAA information is typically stored in an external database or remote server such as a RADIUS or TACACS+ server. The information can also be stored locally on the access server or router.

Remote security servers, such as RADIUS and TACACS+ servers, assign users specific privileges by associating attribute-value pairs, which define the access rights with the appropriate user. All authorization methods must be defined through AAA.

### About RADIUS Authentication and Authorization

*Authentication* is the process by which a system or network verifies the identity of a user who wishes to access it. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual—that is the role of authorization.

*Authorization* is the process of giving individuals specific access rights to system or network resources based on their identity. Authorization employs *access control rules* to determine whether access requests from authenticated users are approved (granted) or disapproved (rejected).

The RADIUS protocol combines user authentication and authorization steps into one phase. The user must be successfully authenticated before the RADIUS server sends authorization information (from the user's profile) to the Network Access Server (NAS).

Commands authorization assigns a list of CLI commands that can be executed by a specified user. The permitted CLI commands are defined on the remote RADIUS server in a user's profile.

When authentication is successful, the RADIUS server returns the permitted list of CLI commands that the authenticated user is authorized to execute. By default, all users can execute a minimal set of commands regardless of their authorization status, for example, "exit" and "logout."

This minimal set of commands can prevent deadlock on the switch due to an error in the user's authorization profile on the RADIUS server.

The user's profile is encoded into Vendor-Specific Attributes (VSAs).

The list of permitted commands is used to filter all the commands executed by the user until the end of the session. This allows greater authorization control, where different rights can be given to different manager or operator users.

## About the RADIUS Protocol

The RADIUS (Remote Authentication Dial-In User Service) protocol carries authentication, authorization, and configuration information between a network access server (NAS) and a RADIUS authentication server.

Authentication with RADIUS allows for a unique password for each user, instead of the need to maintain and distribute switch-specific passwords to all users. RADIUS verifies identity for the following types of primary password access to the switch:

- Serial port (console)
- Telnet
- SSH
- SFTP/SCP
- WebAgent
- Port-Access (802.1X)

ArubaOS switches support RADIUS accounting for web-based authentication and MAC authentication sessions, collecting resource consumption data and forwarding it to the RADIUS server. This data can be used for trend analysis, capacity planning, billing, auditing, and cost analysis.

Requests and responses carried by the RADIUS protocol are called RADIUS *attributes*. These attributes provide the information needed by a RADIUS server to authenticate users and to establish authorized network service for them. The RADIUS protocol also carries accounting information between a network access server and a RADIUS accounting server.

RADIUS is a client/server protocol. The RADIUS client is typically a network access server. The client passes user information to designated RADIUS servers and acts on the response that is returned. RADIUS servers receive user connection requests, authenticate the user, and then return the configuration information necessary for the client to deliver service to the user.

## About the TACACS+ Protocol

TACACS AAA systems are used as a single point of management to configure and store user accounts. They are often coupled with directories and management repositories, simplifying the set up and maintenance of the end-user accounts.

In the authorization function of the AAA system, network devices with Authentication Services can provide fine-grained control over user capabilities for the duration of the user's session; for example, setting access control or session duration.

Enforcement of restrictions to a user account can limit available commands and levels of access.

TACACS+ authentication provides a central server in which you can allow or deny access to switches and other TACACS-aware devices in your network. TACACS employs a central database that creates multiple unique user name and password sets with their associated privilege levels. This central database can be accessed by individuals via the ArubaOS switch from either a console port or via Telnet.

TACACS+ uses an authentication hierarchy consisting of:

- Remote passwords assigned in a TACACS+ server
- Local passwords configured on the switch

---

In the event of a connection failure, a TACACS+ server defaults to locally assigned passwords for authentication control.

---



A TACACS+ server is able to:

- Configure login authentication for read/write or read-only privileges.
- Manage the authentication of login attempts by either the console port or via Telnet.

## Setting Up RADIUS Accounting

This section provides the following information:

- [Accounting Services](#)
- [RADIUS Accounting Server](#)
- [Enabling RADIUS Accounting](#)
- [Operating Rules for RADIUS Accounting](#)
- [Operating Rules for RADIUS](#)

### Accounting Services

RADIUS accounting on the switch collects resource consumption data and forwards it to the RADIUS server. This data can be used for trend analysis, capacity planning, billing, auditing, and cost analysis. Accounting support is provided for WebAgent sessions on the switch.

RADIUS accounting collects data about user activity and system events and sends it to a RADIUS server when specified events occur on the switch, such as a logoff or a reboot.

### Accounting Service Types

The switch supports four types of accounting services:

- Network accounting
  - Provides records containing information on clients directly connected to the switch and operating under Port-Based Access Control (802.1X).
- Executive accounting
  - Provides records holding the information about login sessions (console, Telnet, and SSH) on the switch.
- System accounting
  - Provides information regarding system events that occur on the switch, including system reset, system boot, and enabling or disabling system accounting.
- Commands accounting
  - Provides records containing information on CLI-command execution during user sessions.

## RADIUS Accounting Server

A Network Access Server (NAS) operates as a client of the RADIUS accounting server. The client is responsible for passing user accounting information to a designated RADIUS accounting server.

The RADIUS accounting server is responsible for receiving the accounting request and returning a response to the client indicating that it has successfully received the request.

The RADIUS accounting server can act as a proxy client to other kinds of accounting servers. Transactions between the client and RADIUS accounting server are authenticated through the use of a shared secret, which is never sent over the network.

## Enabling RADIUS Accounting

You can enable RADIUS Accounting for multiple features within the switch accounting configuration. Additionally you can configure **accounting start-stop** for other components.

You also need to configure the accounting interval update timer—**aaa accounting update periodic** parameter (set to **2** minutes in the example below).

To set up RADIUS accounting, run the following commands:

```
ArubaOS-switch(config)# aaa accounting network start-stop radius server-group CP-cluster
ArubaOS-switch(config)# aaa accounting update periodic 2
ArubaOS-switch(config)# show accounting
Replace Figure 2 with new screensho: Angel
```

**Figure 146** *show accounting Command Output*

Status and Counters - Accounting Information		
<u>Interval(min)</u> : 2		
<u>Suppress Empty User</u> : No		
<u>Sessions Identification</u> : Unique		
Type	Method Mode	Server Group
Network	Radius Start-Stop	radius
Exec	None	
System	None	
Commands	None	

## Operating Rules for RADIUS Accounting

The operating rules for RADIUS accounting are as follows:

- You can configure up to four types of accounting to run simultaneously: executive, system, network, and command.
- RADIUS servers used for accounting are also used for authentication.
- The switch must be configured to access at least one RADIUS server.
- RADIUS servers are accessed in the order in which their IP addresses were configured in the switch. To view the order of the RADIUS servers, use the **show radius** command.

As long as the first server is accessible and responding to authentication requests from the switch, a second or third server cannot be accessed.

- If access to a RADIUS server fails during a session, but after the client has been authenticated, the switch continues to assume the server is available to receive accounting data. Thus, if server access fails during a session, it doesn't receive accounting data transmitted from the switch.

## Operating Rules for RADIUS

The ArubaOS switch operating rules for RADIUS are as follows:

- You must have at least one RADIUS server accessible to the switch.
- The switch supports authentication and accounting using up to fifteen RADIUS servers. The switch accesses the servers in the order in which they are listed by show radius. If the first server does not respond, the switch tries the next one, and so on.
- You can select RADIUS as the primary authentication method for each type of access.




---

Only one primary and one secondary access method is allowed for each access type.

---

- In the switch, EAP RADIUS uses MD5 and TLS to encrypt a response to a challenge from a RADIUS server.
- When primary/secondary authentication is set to **Radius/Local** (for either **Login** or **Enable**) and the RADIUS server fails to respond to a client attempt to authenticate, the failure is noted in the Event Log with the message:

*radius: Can't reach RADIUS server <server-ip-address>.*

When this type of failure occurs, the switch prompts the client again to enter a user name and password. In this case, use the local user name (if any) and password configured on the switch itself.

- Zero-length user names or passwords are not allowed for RADIUS authentication, even though this is allowed by some RADIUS servers.

## Additional Configuration Considerations

Beyond the 802.1X configuration basics described above, there are many additional parameters you may choose to configure across the switch ports, such as the following recommendations.

### Limiting Access for Unauthorized Clients

On the ArubaOS switch, a switch port with a static VLAN ID and an unauthenticated client VLAN ID is automatically part of the Unauthenticated-client VLAN as soon as a device connects. If the device passes authentication, the port becomes an untagged member of the static VLAN. This behavior helps guest and other devices with 802.1X supplicants to connect more quickly.

To set an unauthenticated-client VLAN for one or more interfaces, issue the following command:

```
ArubaOS-switch (config) # aaa port-access authenticator <port ID list> unauth-vid <VLAN ID>
```

The **unauth-vid** parameter configures the VLAN to keep the specified ports while there is an unauthenticated client connected to the network.

### Preventing Connectivity Delays for 802.1X Devices

For users who use 802.1X to log in, setting an unauthenticated-client VLAN might lose connectivity. If the user's device allows non-EAP traffic before authentication, it might receive a DHCP address that is in the unauthenticated-client VLAN, which would cause the user's device to lose connectivity after the port moves to the VLAN for authenticated users.

To prevent connectivity delays based on this scenario, issue the following command:

```
ArubaOS-switch (config) # aaa port-access authenticator <port ID list> unauth-period <seconds>
```

## Authenticating Users to the ArubaOS Switch

This section contains the following information

- [Authenticating Users to the ArubaOS Switch](#)
- [What are the Supported Protocols for ArubaOS Switch Management Authentication and Authorization?](#)
- [What Are the Pros and Cons of TACACS vs RADIUS for Authentication and Authorization?](#)

## Why Use ClearPass to Perform Authentication and Authorization for the ArubaOS Switch?

Using ClearPass for handling authentication to the ArubaOS switch allows for a centralized source of user account information that can be used for controlling access to the ArubaOS switch. This helps to minimize the number of changes that need to be made to the network when switch administrators come and go or change access levels.

In addition to authenticating users, ClearPass can also perform command authorization. Some users logged in as administrators to the ArubaOS switch might only be allowed to send certain commands to the command line interface (CLI) to perform their job functions. With command authorization, each and every command that is entered into the switch CLI is validated against the enforcement policy that ClearPass has assigned to that user.

ClearPass provides a robust platform for defining access policies based on contextual information about the authentication request, as well as orchestration of possible follow-up actions based on the policy outcome.

## What are the Supported Protocols for ArubaOS Switch Management Authentication and Authorization?

The ArubaOS Switch supports authentication and authorization checks to an AAA server using either the TACACS+ or RADIUS protocols. There are some inherent differences between the two protocols that might determine which protocol to choose in a given environment.

## What Are the Pros and Cons of TACACS vs RADIUS for Authentication and Authorization?

## Switch Management Using TACACS+

This section contains the following information:

- [Overview](#)
- [Setting Up Switch Management Using TACACS+](#)
- [Creating Enforcement Profiles to Provide Manager Access and Command Control to the ArubaOS Switch](#)
- [Creating an Enforcement Policy to Define Access to the Switch](#)
- [Creating a Service to Support TACACS+ Authentication Requests from the Switch](#)
- [Setting Up the Switch for Command Authorization Using TACACS+](#)
- [Setting Up Enforcement Profiles in ClearPass to Support TACACS+ Command Authorization Requests from the Switch](#)

### Overview

To use TACACS+ authentication, you need the following:

- A TACACS+ server application installed and configured on one or more servers or management stations in your network.
- An ArubaOS switch configured for TACACS+ authentication, with access to one or more TACACS+ servers.

The effectiveness of TACACS+ security depends on correctly using your TACACS+ server application. For this reason, Hewlett Packard Enterprise recommends that you thoroughly test all TACACS+ configurations used in your network.

TACACS+-aware switches include the capability of configuring multiple backup TACACS+ servers. Hewlett Packard Enterprise recommends that you use a TACACS+ server application that supports a redundant backup installation. This allows you to configure the switch to use a backup TACACS+ server if it loses access to the first-choice TACACS+ server. TACACS+ does not affect WebAgent access.

## Setting Up Switch Management Using TACACS+

This section describes how to set up ArubaOS switch management using TACACS+. The following methods are described:

- SSH (Secure Shell)
- Telnet
- Console

### Initial TACACS+ Management Configuration



Out-of-band management (oobm) is only required if the ArubaOS switch will be using the out-of-band management interface to communicate with the TACACS+ server.

To provide initial TACACS+ management configuration:

1. Define the TACACS+ server in the ArubaOS switch.

```
ArubaOS-switch(config) # tacacs-server host 10.2.97.10 oobm key supersecretkey123
```

2. Optionally, adjust the TACACS+ server timeout period as needed. The default is 3 seconds.

```
ArubaOS-switch(config) # tacacs-server timeout 5
```

3. Configure TACACS+ single login capability.

```
ArubaOS-switch(config) # aaa authentication login privilege-mode
```

### Configuring SSH Login for TACACS+ Authentication

To configure the SSH (Secure Shell) login for TACACS+ authentication:

1. Configure TACACS+ authentication for SSH login with read-only (operator) access:

```
ArubaOS-switch(config) # aaa authentication ssh login tacacs local
```

2. Configure TACACS+ authentication for SSH login with access to privileged (manager) access

```
ArubaOS-switch(config) # aaa authentication ssh enable tacacs local
```

### Configuring Telnet Login for TACACS+ Authentication

To configure the Telnet login for TACACS+ authentication:

1. Configure TACACS+ authentication for Telnet login with read-only (operator) access:

```
ArubaOS-switch(config) # aaa authentication telnet login tacacs local
```

2. Configure TACACS+ authentication for Telnet login with access to privileged (manager) access

```
ArubaOS-switch(config) # aaa authentication telnet enable tacacs local
```

## Configuring the Console Login for TACACS+ Authentication

To configure the Console login for TACACS+ authentication:

1. Configure TACACS authentication for Console login with read-only (operator) access:

```
ArubaOS-switch(config) # aaa authentication console login tacacs local
```

2. Configure TACACS authentication for Console login with access to privileged (manager) access

```
ArubaOS-switch(config) # aaa authentication console enable tacacs local
```

## Creating Enforcement Profiles to Provide Manager Access and Command Control to the ArubaOS Switch

- [Adding Active Directory as an Authentication Source](#)
- [Creating an Enforcement Profile to Provide Manager-Level Access](#)
- [Creating an Enforcement Profile to Provide Operator-Level Access](#)

The service to authenticate TACACS+ users against Active Directory incorporates enforcement profiles that define manager-level access and operator-level access to the ArubaOS switch. For this reason, we recommend that the necessary enforcement profiles be created before the service is created.

### Adding Active Directory as an Authentication Source

Before you create the enforcement profiles as described below, we recommend that you configure Active Directory as an authentication source first, as you will need to specify the authentication source when you create the RADIUS enforcement policy.

For details, see [Adding Active Directory as an Authentication Source to ClearPass on page 157](#).

### Creating an Enforcement Profile to Provide Manager-Level Access

In ClearPass Policy Manager, an enforcement policy provides the rules that tells ClearPass when to use specific enforcement profiles. Enforcement profiles consist of actions that are taken by ClearPass, for example, assigning a certain role to a user.

The actions in an enforcement policy are the enforcement profiles to be activated when specific conditions are met or rules are enforced. Then an enforcement policy is associated with a service—a service ties all the elements together: authentication sources, authorization sources, enforcement policies, and role-mapping.

To create an enforcement profile to provide manager-level access to the ArubaOS switch:

1. On the ClearPass server, navigate to **Configuration > Enforcement > Profiles**.
2. From the **Enforcement Profiles** page, click **Add**.

The **Add Enforcement Profiles** dialog opens.

**Figure 147** Adding a TACACS-Based Enforcement Profile for Manager-Level Access

The screenshot shows the 'Add Enforcement Profile' page under 'Enforcement Profiles'. The 'Profile' tab is selected. The 'Template' dropdown is set to 'TACACS+ Based Enforcement'. The 'Name' field contains 'ArubaOS-Switch-Manager'. The 'Description' field contains 'Provides "manager" level access to the ArubaOS switch.' The 'Type' field is set to 'TACACS'. The 'Action' section has 'Accept' selected. The 'Device Group List' section is empty, with a 'Remove' button and a link to 'Add new Device Group'. At the bottom are 'Back to Enforcement Profiles', 'Next >', 'Save', and 'Cancel' buttons.

3. Specify the **Add Enforcement Profile > Profile** tab parameters as described in the following table, then click **Next**:

**Table 43:** Add TACACS-Based Manager-Level Enforcement Profile > Profile Tab Parameters

Parameter	Action/Description
Template	From the Template drop-down, select <b>TACACS+ Based Enforcement</b> .
Name	Enter the name of this enforcement profile: <b>ArubaOS-Switch-Manager</b> .
Description	Add a description of this enforcement profile: Provides manager-level access to the ArubaOS switch.
Type	When you select <b>TACACS+ Based Enforcement</b> , the enforcement profile Type is set to <b>TACACS</b> .
Action	Set to <b>Accept</b> (the default).

## Services Tab

The next step is to configure the **Services** parameters.

**Figure 148** TACACS+ Enforcement Profile for Manager-Level Access > Services Tab

Configuration > Enforcement > Profiles > Add Enforcement Profile

Enforcement Profiles

Profile Services Commands Summary

Privilege Level: 15 (Privileged)

Selected Services: Shell Remove

Authorize Attribute Status: ADD

Custom Services: To add new TACACS+ services / attributes, upload the modified dictionary xml - [Update TACACS+ Services Dictionary](#)

**Service Attributes**

Type	Name	=	Value
1. Shell	priv-lvl	=	15
2. Click to add...			

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

- Specify the **Add Enforcement Profile > Services** tab parameters as described in the following table, then click **Next**:

**Table 44:** TACACS+ Manager-Level Enforcement Profile > Services Parameters

Parameter	Action/Description
Privilege Level	Select <b>15 (Privileged)</b> .
Selected Services	Select <b>Shell</b> . Within a TACACS+ enforcement profile, TACACS can access services that are available on network access device, such as the ArubaOS switch. On this step, <i>Shell</i> is a service that is available on the switch that this enforcement profile will use.
Authorize Attribute Status	Specify <b>Add</b> (the default).
<b>Service Attributes</b>	
Type	Select <b>Shell</b> .
Name	Select <b>priv-lvl</b> .
Value	Enter a value of <b>15</b> .

## Commands Tab

The next step is to configure the **Commands** parameters.

**Figure 149** TACACS+ Enforcement Profile for Manager-Level Access > Commands Tab

Configuration > Enforcement > Profiles > Add Enforcement Profile  
Enforcement Profiles

Profile Services Commands Summary

Service Type:  Shell  PIX Shell  
Unmatched Commands:  Enable to permit unmatched commands

**Commands**  
Specify which commands with arguments are permitted/denied

Command	Arguments	Permit Action	Unmatched Arguments
			<input type="button" value="Add"/>

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

1. Specify the **Add Enforcement Profile > Commands** tab parameters as described in the following table, then click **Next**:

**Table 45:** Add Enforcement Profile > Commands Parameters

Parameter	Action/Description
Service Type	Select <b>Shell</b> .
Unmatched Commands	Click the check box for <b>Enable to permit unmatched commands</b> .

## Summary Tab

The following figure displays the **Summary** tab for the enforcement profile for manager-level access.

**Figure 150** Summary of the TACACS+ Enforcement Profile for Manager-Level Access

Configuration > Enforcement > Profiles > Add Enforcement Profile  
Enforcement Profiles

Enforcement profile has not been saved

Profile Services Commands Summary

**Profile:**

Template:	TACACS+ Based Enforcement
Name:	ArubaOS-Switch-Manager
Description:	Provides "manager" level access to the ArubaOS Switch
Type:	TACACS
Action:	-
Device Group List:	-

**Services:**

Privilege Level:	15
Selected Services:	1. Shell
Authorize Attribute Status:	ADD
Custom Services:	-

**Service Attributes**

Type	Name	=	Value
1. Shell	priv-lvl	=	15

**Commands:**

Service Type:	shell
Unmatched Commands:	Permit

**Commands**

Command	Arguments	Permit Action	Unmatched Arguments
			<input type="button" value="Add"/>

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

- Click **Save**.

You return to the **Enforcement Profiles** page where you receive the message:  
*Enforcement profile "ArubaOS Switch-Manager" added*

### Creating an Enforcement Profile to Provide Operator-Level Access

To create an enforcement profile to provide operator-level access:

- On the ClearPass server, navigate to **Configuration > Enforcement > Profiles**.
- From the **Enforcement Profiles** page, click **Add**.  
 The **Add Enforcement Profiles** dialog opens.

**Figure 151** Adding a TACACS+ Enforcement Profile for Operator-Level Access

- Specify the **Add Enforcement Profile > Profile** tab parameters as described in the following table:

**Table 46: Add Operator-Level Enforcement Profile > Profile Tab Parameters**

Parameter	Action/Description
Template	From the Template drop-down, select <b>TACACS+ Based Enforcement</b> .
Name	Enter the name of this enforcement profile: <b>ArubaOS-Switch-Operator</b> .
Description	Add a description of this Operator-level enforcement profile: Provides Operator-level access to the ArubaOS switch.
Type	When you select <b>TACACS+ Based Enforcement</b> , the enforcement profile type is set to <b>TACACS</b> .
Action	Set to <b>Accept</b> (the default).

- Click **Next**.

### Services Tab

The **Services** tab opens.

**Figure 152** Add Operator-Level Enforcement Profile > Services Parameters

The screenshot shows the 'Add Enforcement Profile' configuration page with the 'Services' tab selected. The 'Privilege Level' is set to '14'. Under 'Selected Services', 'Shell' is listed with a 'Remove' button. An 'Export All TACACS+ Services Dictionaries' link is available. The 'Authorize Attribute Status' dropdown is set to 'ADD'. A note for 'Custom Services' indicates how to add new TACACS+ services/attributes via XML upload. The 'Service Attributes' section contains a table with one entry: Type 'Shell', Name 'priv-lvl', and Value '14'. Buttons at the bottom include 'Back to Enforcement Profiles', 'Next >', 'Save', and 'Cancel'.

- Specify the **Add Enforcement Profile > Services** tab parameters as described in the following table, then click **Next**:

**Table 47:** Add Operator-Level Enforcement Profile > Services Parameters

Parameter	Action/Description
Privilege Level	Select <b>14</b> .
Selected Service	Select <b>Shell</b> .
Authorize Attribute Status	Specify <b>ADD</b> (the default).
<b>Service Attributes</b>	
Type	Select <b>Shell</b> .
Name	Select <b>priv-lvl</b> .
Value	Enter a value of <b>14</b> .

### Commands Tab

The next step is to configure the enforcement profile **Commands** parameters.

**Figure 153** Enforcement Profile for Operator-Level Access > Commands Tab

- Specify the **Commands** parameters as described in the following table, then click **Next**:

**Table 48:** Add Operator-Level Enforcement Profile > Commands Parameters

Parameter	Action/Description
Service Type	Specify <b>Shell</b> .
Unmatched Commands	Click the check box to <b>Enable to permit unmatched commands</b> .

**Figure 154** Enforcement Profile for Operator-Level Access > Summary Tab

- Click **Save**.

You return to the **Enforcement Profiles** page where you receive the message:

*Enforcement profile "ArubaOS Switch-Operator" added*

## Creating an Enforcement Policy to Define Access to the Switch

The service to authenticate TACACS+ users against Active Directory incorporates an enforcement policy that defines access to the ArubaOS switch. For this reason, we recommend that you create the enforcement policy before the service is created.

To create an enforcement policy to define manager-level and operator-level access to the ArubaOS switch:

1. Navigate to **Configuration > Enforcement > Policies**.
2. From the **Enforcement Policies** page, click **Add**.  
The **Add Enforcement Policy** page opens.

**Figure 155** Defining a Policy for Manager-Level and Operator-Level Access to the Switch

Configuration > Enforcement > Policies > Add  
Enforcement Policies

Enforcement	Rules	Summary
Name: ArubaOS-Switch Management Policy	Description: "Manager" vs. "Operator" level access to the ArubaOS-Switch	
Enforcement Type: <input type="radio"/> RADIUS <input checked="" type="radio"/> TACACS+ <input type="radio"/> WEBAUTH (SNMP/Agent/CLI/CoA) <input type="radio"/> Application <input type="radio"/> Event	Default Profile: [TACACS Deny Profile] <a href="#">View Details</a> <a href="#">Modify</a> <a href="#">Add new Enforcement Profile</a>	

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

3. Specify the **Add Enforcement Policy** parameters as described in the following table, then click **Next**.

**Table 49: Add Enforcement Policy Parameters**

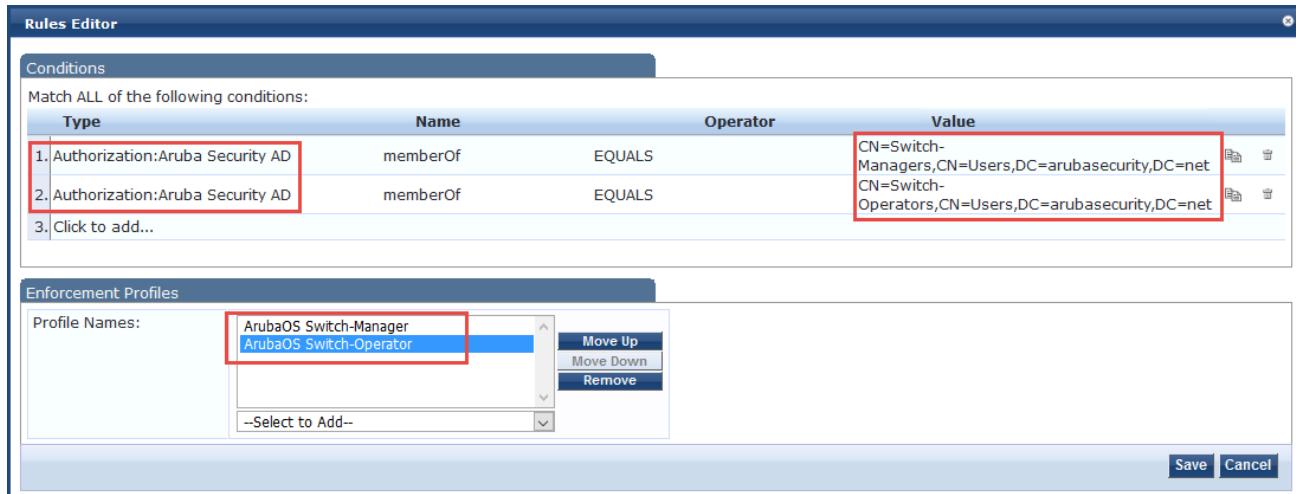
Parameter	Action/Description
Name	Enter a name for this enforcement policy; for example, "ArubaOS-Switch Management Policy."
Description	Optionally (but recommended), add a description of this enforcement policy; for example, "Policy to assign manager vs Operator-level access to the ArubaOS switch."
Enforcement Type	Select <b>TACACS+</b> . Based on this selection, the <b>Default Profile</b> drop-down lists the associated enforcement profiles. In this example, it is the <b>TACACS Deny Profile</b> . <b>NOTE:</b> Web-based Authentication or WebAuth (HTTPS) is the mechanism used by authentications performed via a browser, and authentications performed via ClearPass OnGuard. Both SNMP- and CLI- (SSH/Telnet) based enforcement profiles can be sent to the network device based on the type of device and the use case.
Default Profile	Select <b>ArubaOS Switch Manager</b> . An enforcement policy applies conditions (roles, health, and time attributes) against specific values associated with those attributes to determine the enforcement profile. If none of the rules matches, ClearPass applies the default profile.

Parameter	Action/Description
	To add a new profile, click <b>Add New Enforcement Profile</b> .

When you click **Next**, the **Rules** dialog opens.

4. Click **Add Rule**.
5. The **Rules Editor** opens:

**Figure 156** Add Enforcement Policy > Rules Editor



6. Specify the **Add Enforcement Policy** > **Rules** tab parameters as described in the following table:

**Table 50: Configuring Rules for ArubaOS Switch—Manager and Operator**

Parameter	Action/Description
<b>Conditions</b>	
Type	<ul style="list-style-type: none"> <li>• Manager: Select <b>Authorization:Aruba Security AD</b>.</li> <li>• Operator: Select <b>Authorization:Aruba Security AD</b>.</li> </ul> <p><b>NOTE:</b> The Aruba Security AD authorization source must be added manually. For details, see <a href="#">Adding Active Directory as an Authentication Source to ClearPass on page 157</a>.</p>
Name	<ul style="list-style-type: none"> <li>• Manager: Select <b>memberOf</b>.</li> <li>• Operator: Select <b>memberOf</b>.</li> </ul>
Operator	<ul style="list-style-type: none"> <li>• Manager: Select <b>EQUALS</b>.</li> <li>• Operator: Select <b>EQUALS</b>.</li> </ul>

Parameter	Action/Description
Value	<ul style="list-style-type: none"> <li>Manager: Enter <b>CN=Switch-Managers,CN=Users,DC=arubasecurity,DC=net</b>.</li> <li>Operator: Enter <b>CN=Switch-Operators,CN=Users,DC=arubasecurity,DC=net</b>.</li> </ul>
<b>Enforcement Profiles</b>	
Profile Names	<ul style="list-style-type: none"> <li>Manager: Select <b>ArubaOS Switch-Manager</b>.</li> <li>Operator: Select <b>ArubaOS Switch-Operator</b>.</li> </ul>

7. Click **Save**.

You return to the **Add Enforcement Policies > Rules** page, where the new enforcement rules are displayed:

**Figure 157 ArubaOS Switch Manager and Operator Enforcement Policy Rules**

The screenshot shows the 'Rules' tab selected in the 'Enforcement Policies' interface. A single rule is listed:

```

Conditions: (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-Managers,CN=Users,DC=arubasecurity,DC=net)
Actions: ArubaOS Switch-Manager, ArubaOS Switch-Operator
1. AND (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-Operators,CN=Users,DC=arubasecurity,DC=net)
  
```

Buttons at the bottom include 'Add Rule', 'Move Up', 'Move Down', 'Edit Rule', and 'Remove Rule'.

8. Click **Next**.

The **Add Enforcement Policies > Summary** page opens:

**Figure 158 ArubaOS TACACS+ Enforcement Policy Summary**

The screenshot shows the 'Summary' tab selected. The enforcement policy details are:

**Enforcement:**

- Name: ArubaOS Switch Mgmt Enforcement Policy
- Description: Policy to assign manager- vs operator-level access to the ArubaOS switch
- Enforcement Type: TACACS
- Default Profile: ArubaOS Switch-Manager

**Rules:**

Rules Evaluation Algorithm: First applicable

Conditions	Actions
(Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-Managers,CN=Users,DC=arubasecurity,DC=net)	ArubaOS Switch-Manager, ArubaOS Switch-Operator
1. AND (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-Operators,CN=Users,DC=arubasecurity,DC=net)	ArubaOS Switch-Manager, ArubaOS Switch-Operator

9. Click **Save**.

You return to the **Enforcement Policies** page where the following message is displayed:

*Enforcement policy "ArubaOS Switch Mgmt Enforcement Policy" has been added.*

## Creating a Service to Support TACACS+ Authentication Requests from the Switch

The service to support TACACS+ authentication requests from the ArubaOS switch incorporates the previously-created elements:

- Enforcement profiles that define manager-level access and operator-level access to the ArubaOS switch (see [Creating Enforcement Profiles to Provide Manager Access and Command Control to the ArubaOS Switch on page 198](#)).
- Enforcement policy that defines access to the ArubaOS switch (see [Creating an Enforcement Policy to Define Access to the Switch on page 205](#)).

To create a service to authenticate TACACS+ users against Active Directory:

1. Navigate to **Configuration > Services**.
  2. From the **Services** page, click the **Add** link.
- The **Add Configuration Services** page opens.

**Figure 159** Adding a TACACS+ Enforcement Service

The screenshot shows the 'Add Configuration Services' page with the following details:

- Type:** TACACS+ Enforcement
- Name:** ArubaOS Switch Management
- Description:** Service to authenticate TACACS+ users against Active Directory
- Monitor Mode:**  Enable to monitor network access without enforcement
- More Options:**  Authorization

**Service Rule**

Matches  ANY or  ALL of the following conditions:

Type	Name	Operator	Value
1. Connection	NAD-IP-Address	EQUALS	10.
2. Connection	Protocol	EQUALS	TACACS
3. Click to add...			

A red callout box with the text "IP address of the ArubaOS switch" points to the value "10." in the "Value" column of the first row of the table.

- The service rule states that if the NAD-IP-Address value in the TACACS request = the IP address value specified in the **Value** parameter.
  - And if the protocol of the request = TACACS, the TACACS+ request will match the TACACS+ Enforcement service.
3. Specify the **Add TACACS+ Enforcement Service** parameters as described in the following table:

**Table 51: Add TACACS+ Enforcement Service Parameters**

Parameter	Action/Description
Type	Select <b>TACACS+ Enforcement</b> .
Name	Enter a name for this service.
Description	Optionally (but recommended), add a description of this enforcement service.
Monitor Mode	This option is disabled by default. Do not enable Monitor Mode.
More Options	Click the check box to enable <b>Authorization</b> .

Parameter	Action/Description
<b>Service Rule</b>	
Matches	Select <b>All of the following conditions</b> .
<i>Rule condition 1: Connecting to the Active Directory server</i>	Select <b>Click to add</b> , then specify the following attributes: <ul style="list-style-type: none"> <li>• Type: <b>Connection</b></li> <li>• Name: <b>NAD-IP-Address</b></li> <li>• Operator: <b>EQUALS</b></li> <li>• Value: &lt;IP address of the ArubaOS switch&gt;</li> </ul>
<i>Rule condition 2: Specifying the TACACS+ protocol</i>	Select <b>Click to add</b> , then specify the following attributes: <ul style="list-style-type: none"> <li>• Type: <b>Connection</b></li> <li>• Name: <b>Protocol</b></li> <li>• Operator: <b>EQUALS</b></li> <li>• Value: <b>TACACS</b></li> </ul>

4. Click **Next**.

The **Authentication** tab opens.

**Figure 160** TACACS+ Enforcement Service > Authentication Tab

5. From the **Authentication Sources** drop-down, select **Aruba Security AD** (or whatever name was assigned to this authentication source), then click **Next**.

The **Authorization** tab opens.

**Figure 161 TACACS+ Enforcement Service > Authorization Tab**

The screenshot shows the 'Authorization' tab selected in a service configuration window. It displays two sections: 'Authorization Details' and 'Additional authorization sources from which to fetch role-mapping attributes'. In the 'Authorization Details' section, there is a table with one row showing 'Aruba Security AD [Active Directory]' as the authentication source and 'Aruba Security AD [Active Directory]' as the source for fetched attributes. Below this is a dropdown menu with options 'Remove', 'View Details', and 'Modify'. The 'Additional authorization sources' section contains a list with 'Aruba Security AD [Active Directory]' and a 'Select to Add...' button. At the bottom are 'Back to Services', 'Next >', 'Save', and 'Cancel' buttons.

6. From the *Additional authorization sources from which to fetch role-mapping attributes* drop-down, select **Aruba Security AD (Active Directory)**.
7. Select the **Enforcement** tab.

**Figure 162 TACACS+ Enforcement Service > Enforcement Tab**

The screenshot shows the 'Enforcement' tab selected in a service configuration window. It includes sections for 'Use Cached Results', 'Enforcement Policy', and 'Enforcement Policy Details'. Under 'Enforcement Policy Details', there is a table with columns 'Conditions' and 'Enforcement Profiles'. The 'Conditions' column lists a rule: '1. (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-Managers,CN=Users,DC=arubasecurity,DC=net) AND (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-Operators,CN=Users,DC=arubasecurity,DC=net)'. The 'Enforcement Profiles' column lists 'ArubaOS Switch-Manager, ArubaOS Switch-Operator'. At the bottom are 'Add new Enforcement Policy', 'Description', 'Default Profile', and 'Rules Evaluation Algorithm' fields.

8. From the **Enforcement Policy** drop-down, select **ArubaOS Switch Mgmt Enforcement Policy**.
9. Click **Save**.

This completes the service for ArubaOS switch management.

## Setting Up the Switch for Command Authorization Using TACACS+

- [Enabling TACACS+ Command Authorization on the Switch](#)
- [Setting Up Enforcement Profiles in ClearPass to Support TACACS+ Command Authorization Requests from the Switch](#)

### Enabling TACACS+ Command Authorization on the Switch

From the ArubaOS switch, enable command authorization using the same protocol that authentication used:

```
ArubaOS-Switch (config) # aaa authorization commands auto
```

### Setting Up Enforcement Profiles in ClearPass to Support TACACS+ Command Authorization Requests from the Switch

On the ClearPass server, implementing command authorization using TACACS+ is achieved by creating an enforcement profile that defines commands that are either allowed or denied.

The sample enforcement profile created here will permit all commands to be run on the switch, except for those under the AAA configuration hierarchy. This is useful for situations in which the user's role does not include making changes to anything related to authentication, authorization, or accounting.

To set up enforcement profiles in ClearPass to support TACACS+ command authorization requests from the ArubaOS switch:

1. Navigate to **Configuration > Enforcement > Profiles**.

The **Enforcement Profiles** page opens.

2. Click the **Add** link.

The **Add Enforcement Profile** page opens.

**Figure 163** Adding a TACACS+ Command Authorization Enforcement Profile

Configuration > Enforcement > Profiles > Add Enforcement Profile

Enforcement Profiles

**Profile**   **Services**   **Summary**

Template: TACACS+ Based Enforcement

Name: ArubaOS-Switch-NetEng

Description: This profile prohibits access to the "AAA" commands on the switch.

Type: TACACS

Action:  Accept  Reject  Drop

Device Group List:     
--Select--

[Add new Device Group](#)

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

3. Specify the **TACACS+-Based Enforcement Profile** parameters as described in the following table:

**Table 52: Add TACACS+ Enforcement Profile Parameters**

Parameter	Action/Description
Template	Select <b>TACACS+-Based Enforcement</b> .
Name	Enter a name for this enforcement profile.
Description	Optionally (but recommended), add a description of this enforcement profile.
Type	When you select the <i>TACACS+-Based Enforcement</i> template, the enforcement profile <b>Type</b> is set automatically to <b>TACACS</b> .
Action	Keep the default action: <b>Accept</b> .
Device Group List	The <b>Device Group List</b> is no longer pertinent and this option is grayed out.

4. Click **Next**.

#### Add Enforcement Profile > Services Tab

When you click **Next**, the **Services** tab opens.

**Figure 164** Add TACACS+ Enforcement Profile > Services Tab

The screenshot shows the 'Add Enforcement Profile' dialog with the 'Services' tab selected. Key fields include:

- Privilege Level: 15 (Privileged)
- Selected Services: Shell (selected from a dropdown menu)
- Authorize Attribute Status: ADD
- Custom Services: To add new TACACS+ services / attributes, upload the modified dictionary xml - [Update TACACS+ Services Dictionary](#)
- Service Attributes table:
 

Type	Name	=	Value
1. Shell	priv-lvl	=	15
2. Click to add...			

Buttons at the bottom include: Back to Enforcement Profiles, Next >, Save, and Cancel.

- Specify the **TACACS+-Based Enforcement Profile > Services** parameters as described in the following table:

**Table 53:** Add TACACS+ Enforcement Profile > Services Parameters

Parameter	Action/Description
Privilege Level	Select <b>15 (Privileged)</b> .
Selected Services	From the <b>Select</b> drop-down, choose <b>Shell</b> .
Authorize Attribute Status	Specify <b>ADD</b> (which is the default).
Custom Services	When you select the <i>TACACS+-Based Enforcement</i> template, the enforcement profile <b>Type</b> is set automatically to <b>TACACS</b> .
<b>Service Attributes</b>	
Type	Click <b>Click to add</b> , then select <b>Shell</b> .
Name	Select <b>priv-lvl</b> .
Value	Enter a value of <b>15</b> .

- Click **Next**.

#### Add Enforcement Profile > Commands Tab

When you click **Next**, the **Commands** tab opens.

**Figure 165** Add TACACS+ Enforcement Profile > Commands Tab

Configuration > Enforcement > Profiles > Add Enforcement Profile

**Enforcement Profiles**

**Commands Tab**

Service Type:  Shell  PIX Shell

Unmatched Commands:  Enable to permit unmatched commands

Specify which commands with arguments are permitted/denied

Command	Arguments	Permit Action	Unmatched Arguments
			<b>Add</b>

- Specify the **TACACS+-Based Enforcement Profile > Commands** parameters as described in the following table:

**Table 54:** Add TACACS+ Enforcement Profile > Commands Parameters

Parameter	Action/Description
Service Type	The <b>Service Type</b> is automatically set to <b>Shell</b> .
Unmatched Commands	Select the check box to permit unmatched records.

- From the **Commands** panel, click **Add**.

The **Configure TACACS+ Command Authorization** configuration dialog opens.

**Figure 166** Configuring TACACS+ Command Authorization

**Configure TACACS+ Command Authorization**

Shell Command: aaa

Command Arguments	Action
1. *	<input type="checkbox"/> Enable to permit
2. Click to add...	

Unmatched Arguments:  Permit  Deny

**Save** **Cancel**

- Specify the **TACACS+-Based Enforcement Profile > Commands** parameters as described in the following table:

**Table 55: Add TACACS+ Enforcement Profile > Commands Parameters**

Parameter	Action/Description
Shell Command	The <b>Service Type</b> is automatically set to <b>Shell</b> .
Command Arguments	Select <b>Click to add</b> , then enter .*
	By entering a period and an asterisk (*), any string that follows the shell command listed in the <i>Shell Command</i> field will be matched against the enforcement policy.
Action	Do not enable to permit—leave the check box unchecked.
Unmatched Arguments	Select <b>Deny</b> .

10. Click **Save**.

You return to the **Commands** page where it shows that the **aaa** command requests to the ClearPass server from the ArubaOS switch are denied.

**Figure 167 ArubaOS Command Denied**

Command	Arguments	Permit Action	Unmatched Arguments
1. aaa	.*	Deny	

11. Click **Save**.

This enforcement profile is added to the **Enforcement Profiles** page.

## Switch Management Using RADIUS

This section contains the following information

- [Setting Up Switch Management Using RADIUS](#)
- [Using RADIUS-Based Authentication and Command Authorization](#)
- [Creating Enforcement Profiles to Provide Manager Access and Command Authorization to the ArubaOS Switch](#)
- [Creating an Enforcement Policy to Define Access to the Switch](#)

### Setting Up Switch Management Using RADIUS

This section describes how to set up ArubaOS switch management using RADIUS. The following login methods are described:

- Initial
- SSH
- Telnet
- Console
- Web Agent

## Initial RADIUS Management Configuration



Out-of-band management (oobm) is only required if the ArubaOS switch will be using the out-of-band management interface to communicate with the RADIUS server.

To provide initial RADIUS management configuration:

1. Define the RADIUS server in the ArubaOS switch:

```
ArubaOS-switch(config)#radius-server host 10.x.x.x oobm key supersecretkey123
```

2. Optionally, adjust the RADIUS server timeout period as needed. The default is 3 seconds.

```
ArubaOS-switch(config)#radius-server timeout 30
```

3. Configure RADIUS single login capability:

```
ArubaOS-switch(config)#aaa authentication login privilege-mode
```

## Configuring SSH Login for RADIUS Authentication

To configure the SSH (Secure Shell) login for RADIUS authentication:

1. Configure RADIUS authentication for SSH login with read-only (operator) access:

```
ArubaOS-switch(config)#aaa authentication ssh login radius local
```

2. Configure RADIUS authentication for SSH login with access to privileged (manager) access:

```
ArubaOS-switch(config)#aaa authentication ssh enable radius local
```

## Configuring Telnet Login for RADIUS Authentication

To configure the Telnet login for RADIUS authentication:

1. Configure RADIUS authentication for Telnet login with read-only (operator) access:

```
ArubaOS-switch(config)#aaa authentication telnet login radius local
```

2. Configure RADIUS authentication for Telnet login with access to privileged (manager) access:

```
ArubaOS-switch(config)#aaa authentication telnet enable radius local
```

## Configuring the Console Login for RADIUS Authentication

To configure the Console login for RADIUS authentication:

1. Configure RADIUS authentication for the Console login with read-only (operator) access:

```
ArubaOS-switch(config)# aaa authentication console login radius local
```

2. Configure RADIUS authentication for the Console login with access to privileged (manager) access:

```
ArubaOS-switch(config)#aaa authentication console enable radius local
```

## Configuring Web Agent Login for RADIUS Authentication

1. Configure Web Agent authentication for the Web Agent login with read-only (operator) access:

```
Aruba-Stack-3810M(config)# aaa authentication web login radius local
```

- Configure RADIUS authentication for the Web Agent login with access to privileged (manager) access:

```
Aruba-Stack-3810M(config)# aaa authentication web enable radius local
```

## Using RADIUS-Based Authentication and Command Authorization

When using RADIUS-based command authorization on an ArubaOS switch, the list of commands that the user is authorized to run are supplied at authentication time. This is in contrast to TACACS+, where each command being run by the user is sent to the AAA server to be authorized.

The RADIUS-based method of command authorization requires less overhead on the AAA server and affords higher performance in environments that have many concurrent management sessions on the switches.

The examples in the following section describe the following:

- Both Manager and "ViewOnly" levels of access are actually the same as far as the ArubaOS switch is concerned, with the only difference being which commands can be run.
- The Manager-level of access still has command authorization as a RADIUS Vendor Specific Attribute (VSA), but there is no list of commands accompanying that role. When there is no list of commands, all commands can be run.
- The ViewOnly-level of access has command authorization as a RADIUS Vendor Specific Attribute (VSA) and a command list with a regular expression indicating that only commands that begin with the word "show" may be run.

## Creating Enforcement Profiles to Provide Manager Access and Command Authorization to the ArubaOS Switch

The service to authenticate RADIUS users against Active Directory incorporates enforcement profiles that define manager-level access and command authorization to the ArubaOS switch. For this reason, we recommend that the necessary enforcement profiles be created before the service is created.

- [Adding Active Directory as an Authentication Source](#)
- [Creating an Enforcement Profile to Provide Manager-Level Access](#)
- [Creating an Enforcement Profile to Provide Command Authorization](#)

### Adding Active Directory as an Authentication Source

Before you create the enforcement profiles as described below, we recommend that you configure Active Directory as an authentication source first, as you will need to specify the authentication source when you create the RADIUS enforcement policy.

For details, see [Adding Active Directory as an Authentication Source to ClearPass on page 157](#).

### Creating an Enforcement Profile to Provide Manager-Level Access

In ClearPass Policy Manager, an enforcement policy provides the rules that tells ClearPass when to use specific enforcement profiles. Enforcement profiles consist of actions that are taken by ClearPass, for example, assigning a certain role to a user.

The actions in an enforcement policy are the enforcement profiles to be activated when specific conditions are met or rules are enforced. Then an enforcement policy is associated with a service—a service ties all the elements together: authentication sources, authorization sources, enforcement policies, and role-mapping.

To create an enforcement profile to provide manager-level access to the ArubaOS switch:

- On the ClearPass server, navigate to **Configuration > Enforcement > Profiles**.
- From the **Enforcement Profiles** page, click **Add**.

The **Add Enforcement Profiles** dialog opens.

**Figure 168** Adding an Enforcement Profile for Manager-Level Access

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Profile	Attributes	Summary
Template:	RADIUS Based Enforcement	
Name:	ArubaOS-Switch-Manager	
Description:	RADIUS based enforcement policy giving "manager" level access	
Type:	RADIUS	
Action:	<input checked="" type="radio"/> Accept <input type="radio"/> Reject <input type="radio"/> Drop	
Device Group List:	<input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="Modify"/> --Select--	<a href="#">Add new Device Group</a>

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

- Specify the **Add Enforcement Profile > Profile** tab parameters as described in the following table, then click **Next**:

**Table 56:** Add Manager-Level Enforcement Profile > Profile Tab Parameters

Parameter	Action/Description
Template	From the Template drop-down, select <b>RADIUS Based Enforcement</b> .
Name	Enter the name of this enforcement profile: <b>ArubaOS-Switch-Manager</b> .
Description	Add a description of this enforcement profile: Provides manager-level access to the ArubaOS switch.
Type	When you select <b>RADIUS Based Enforcement</b> , the enforcement profile Type is set to <b>RADIUS</b> .
Action	Set to <b>Accept</b> (the default).

### Specifying Enforcement Profile Attributes

- From the Enforcement Profiles **Attributes** tab, select **Click to add**.

**Figure 169** Enforcement Profile for Manager-Level Access >Specifying Attributes

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Type	Name	Value
1. Radius:IETF	Service-Type	= Administrative-User (6)
2. Radius:Hewlett-Packard-Enterprise	HPE-Command-Exception	= Deny-List (1)
3. Click to add...		

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

- Specify the **Add Enforcement Profile > Attributes** as described in the following table:

**Table 57: Manager-Level Enforcement Profile > Attributes**

Attribute	Action/Description
<b>Service-Type Attribute</b>	
Type	Select <b>Radius:IETF</b> .
Name	Select <b>Service-Type</b> .
Value	Select <b>Administrative-User (6)</b> . The value of the <b>Administrative-user</b> parameter is <b>6</b> , which instructs the ArubaOS switch to grant the user manager-level access.
<b>Service-Type Attribute</b>	
Type	Select <b>Radius: Hewlett-Packard_Enterprise</b>
Name	Select <b>HPE-Command-Exception</b>
Value	Select <b>Deny-List</b> <b>HPE-Command-Exception</b> is a flag that specifies whether the commands indicated by the <b>HPE-Command-String</b> attribute are permitted or denied to the user. A zero (0) means permit all listed commands and deny all others; a one (1) means deny all listed commands and permit all others. By adding a value of 1 with no corresponding HPE-Command-String VSA, the user can run all commands.

3. Click **Next**:

The **Summary** for the RADIUS enforcement profile for manager-level access is displayed.

**Figure 170 Summary of the RADIUS Enforcement Profile for Manager-Level Access**

Configuration » Enforcement » Profiles » Add Enforcement Profile

Enforcement Profiles

Enforcement profile has not been saved

Profile	Attributes	Summary									
<b>Profile:</b> Template: RADIUS Based Enforcement Name: ArubaOS-Switch-Manager Description: RADIUS based enforcement policy giving "manager" level access Type: RADIUS Action: Accept Device Group List: -	<b>Attributes:</b> <table border="1"><thead><tr><th>Type</th><th>Name</th><th>Value</th></tr></thead><tbody><tr><td>1. Radius:IETF</td><td>Service-Type</td><td>= Administrative-User (6)</td></tr><tr><td>2. Radius:Hewlett-Packard-Enterprise</td><td>HPE-Command-Exception</td><td>= Deny-List (1)</td></tr></tbody></table>	Type	Name	Value	1. Radius:IETF	Service-Type	= Administrative-User (6)	2. Radius:Hewlett-Packard-Enterprise	HPE-Command-Exception	= Deny-List (1)	
Type	Name	Value									
1. Radius:IETF	Service-Type	= Administrative-User (6)									
2. Radius:Hewlett-Packard-Enterprise	HPE-Command-Exception	= Deny-List (1)									

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

4. Click **Save**.

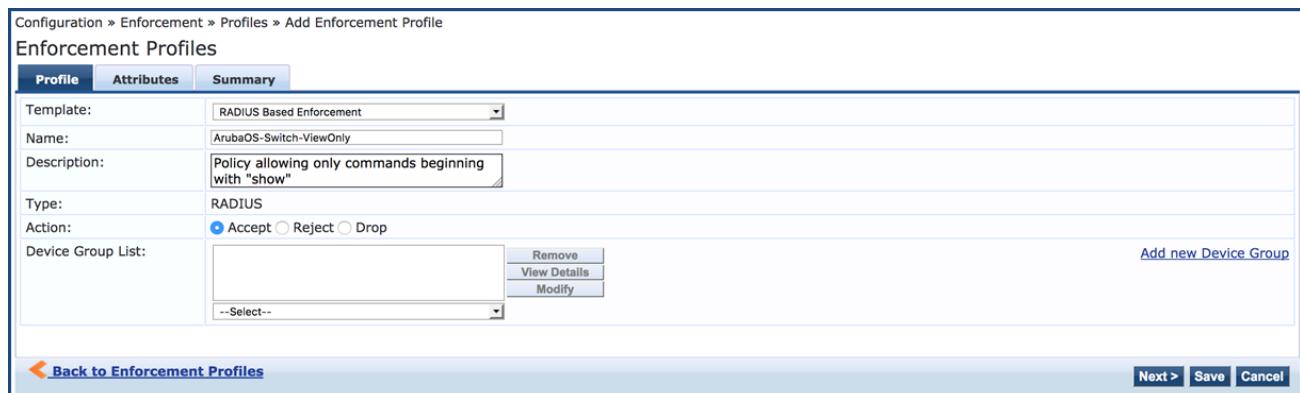
You return to the **Enforcement Profiles** page where you receive the message:  
*Enforcement profile "ArubaOS Switch-Manager" added*

## Creating an Enforcement Profile to Provide Command Authorization

To create a RADIUS-based enforcement profile to provide command authorization:

1. On the ClearPass server, navigate to **Configuration > Enforcement > Profiles**.
2. From the **Enforcement Profiles** page, click **Add**.  
The **Add Enforcement Profiles** dialog opens.

**Figure 171** Adding a RADIUS Enforcement Profile for Command Authorization



The screenshot shows the 'Add Enforcement Profile' dialog box. At the top, there are three tabs: 'Profile' (which is selected), 'Attributes', and 'Summary'. Below the tabs, the 'Template' dropdown is set to 'RADIUS Based Enforcement'. The 'Name' field contains 'ArubaOS-Switch-ViewOnly'. The 'Description' field contains 'Policy allowing only commands beginning with "show"'. Under 'Type', it is set to 'RADIUS'. Under 'Action', the radio button for 'Accept' is selected. The 'Device Group List' section shows a single entry 'ArubaOS-Switch-ViewOnly' with options to 'Remove', 'View Details', or 'Modify'. A link 'Add new Device Group' is available. At the bottom left is a 'Back to Enforcement Profiles' link, and at the bottom right are 'Next >', 'Save', and 'Cancel' buttons.

3. Specify the **Add Enforcement Profile > Profile** tab parameters as described in the following table:

**Table 58:** RADIUS Enforcement Profile > Profile Tab Parameters

Parameter	Action/Description
Template	From the Template drop-down, select <b>RADIUS Based Enforcement</b> .
Name	Enter the name of this enforcement profile: <b>ArubaOS-Switch-ViewOnly</b> .
Description	Add a description of this command control enforcement profile: Policy allowing only commands beginning with "show."
Type	When you select <b>RADIUS Based Enforcement</b> , the enforcement profile type is set to <b>RADIUS</b> .
Action	Set to <b>Accept</b> (the default).

## Specifying Enforcement Profile Attributes

- From the Enforcement Profiles **Attributes** tab, select **Click to add...**.

**Figure 172 Specifying Command Control Attributes**

Configuration » Enforcement » Profiles » Add Enforcement Profile  
Enforcement Profiles

Type	Name	Value
1. Radius:IETF	Service-Type	= Administrative-User (6)
2. Radius:Hewlett-Packard-Enterprise	HPE-Command-Exception	= Permit-List (0)
3. Radius:Hewlett-Packard-Enterprise	HPE-Command-String	= ^show
4. Click to add...		

Back to Enforcement Profiles      Next >      Save      Cancel

- Specify the **Add Enforcement Profile > Attributes** as described in the following table:

**Table 59: Manager-Level Enforcement Profile > Attributes**

Attribute	Action/Description
<b>Service-Type</b>	
Type	Select <b>Radius:IETF</b> .
Name	Select <b>Service-Type</b> .
Value	Select <b>Administrative-User (6)</b> . The value of the <b>Administrative-user</b> parameter is <b>6</b> , which instructs the ArubaOS switch to grant the user manager-level access.
<b>HPE-Command Exception</b>	
Type	Select <b>Radius: Hewlett-Packard_Enterprise</b> .
Name	Select <b>HPE-Command-Exception</b> .
Value	Select <b>Permit-List</b> .
<b>HPE-Command String</b>	

Attribute	Action/Description
Type	Select <b>Radius: Hewlett-Packard Enterprise</b> .
Name	Select <b>HPE-Command String</b> .
Value	<p>Enter <b>^show</b></p> <p><b>HPE-Command-String</b> is a list of commands (regular expressions) that are permitted or denied execution by the user. The commands are delimited by semicolons and must be between 1 and 249 characters in length. Multiple instances of this attribute can be present in Access-Accept packets. (A single instance can be present in Accounting-Request packets.) In this example, the regular expression <b>^show</b> means that commands that begin with the word "show" are allowed. All other commands are denied.</p>

3. Click **Next**:

The **Summary** for the RADIUS enforcement profile for command authorization is displayed.

**Figure 173 Summary of the RADIUS Enforcement Profile for Command Authorization**

Type	Name	Value
Radius:1ETF	Service-Type	= Administrative-User (6)
Radius:Hewlett-Packard-Enterprise	HPE-Command-Exception	= Permit-List (0)
Radius:Hewlett-Packard-Enterprise	HPE-Command-String	= ^show

4. Click **Save**.

You return to the **Enforcement Profiles** page where you receive the message:

*Enforcement profile "ArubaOS Switch-ViewOnly" added*

## Creating an Enforcement Policy to Define Access to the Switch

The service to authenticate RADIUS users against Active Directory incorporates an enforcement policy that defines access to the ArubaOS switch. For this reason, we recommend that you create the enforcement policy before the service is created.

To create an enforcement policy to define manager-level access and command authorization to the ArubaOS switch:

1. Navigate to **Configuration > Enforcement > Policies**.
2. From the **Enforcement Policies** page, click **Add**.

The **Add Enforcement Policy** page opens.

**Figure 174** Defining an Enforcement Policy for the ArubaOS Switch

The screenshot shows the 'Enforcement Policies' configuration interface. The 'Add' tab is selected. The 'Name' field contains 'ArubaOS-Switch-RADIUS-Policy'. The 'Description' field contains 'Enforcement policy for ArubaOS-Switch'. The 'Enforcement Type' section has 'RADIUS' selected. The 'Default Profile' dropdown is set to 'Deny Access Profile'. There are buttons for 'View Details', 'Modify', and 'Add new Enforcement Profile'. At the bottom are 'Back to Enforcement Policies', 'Next >', 'Save', and 'Cancel' buttons.

- Specify the **Add Enforcement Policy** parameters as described in the following table, then click **Next**.

**Table 60:** Add RADIUS Enforcement Policy Parameters

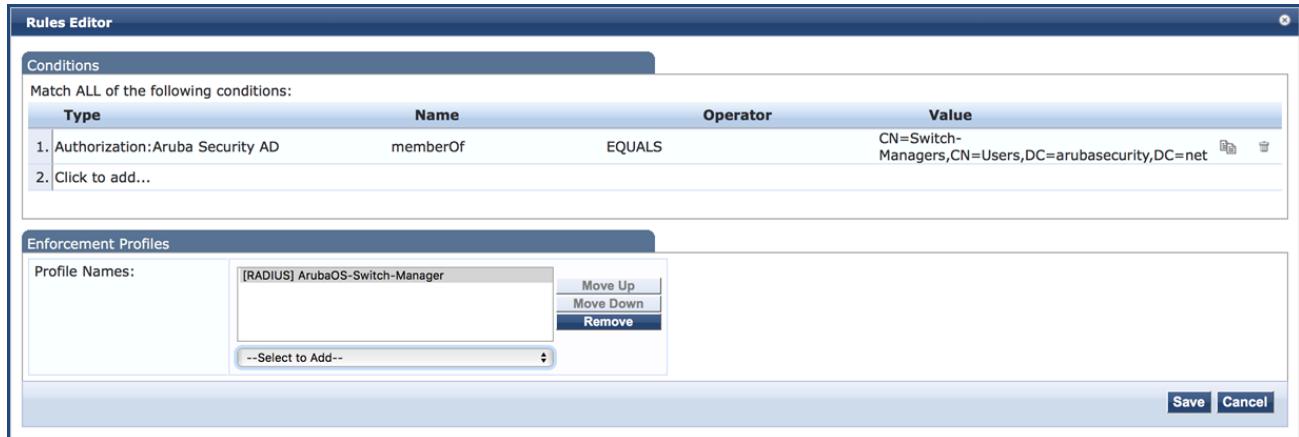
Parameter	Action/Description
Name	Enter a name for this enforcement policy; for example, "ArubaOS-Switch-RADIUS-Policy."
Description	Optionally (but recommended), add a description of this enforcement policy; for example, " Enforcement policy for ArubaOS switch."
Enforcement Type	Select <b>RADIUS</b> . Based on this selection, the <b>Default Profile</b> drop-down lists the associated enforcement profiles.
Default Profile	Select the <b>Deny Access Profile</b> . An enforcement policy applies conditions (roles, health, and time attributes) against specific values associated with those attributes to determine the enforcement profile. If none of the rules matches, ClearPass applies the default profile. To add a new profile, click <b>Add New Enforcement Profile</b> .

When you click **Next**, the **Rules** dialog opens.

- Click **Add Rule**.

The **Rules Editor** opens.

**Figure 175 Rules Editor**



- Specify the **Rules Editor** parameters as described in the following table:

**Table 61: Configuring Rules for ArubaOS Switch—Manager and ViewOnly**

Parameter	Action/Description
<b>Conditions</b>	
Type	<ul style="list-style-type: none"> <li><b>Manager:</b> Specify the authorization source that was created for your Active Directory domain. In this example, the name of the authorization source is <b>Authorization:Aruba Security AD</b>.</li> </ul> <p><b>NOTE:</b> The authorization source must be added manually. For details, see <a href="#">Adding Active Directory as an Authentication Source to ClearPass on page 157</a>.</p>
Name	<ul style="list-style-type: none"> <li><b>Manager:</b> Select <b>memberOf</b>.</li> </ul>
Operator	<ul style="list-style-type: none"> <li><b>Manager:</b> Select <b>EQUALS</b>.</li> </ul>
Value	<p>Fill out the Active Directory Distinguished Name (DN) of the group that contains the user who will be subjected to the enforcement profile below. For example:</p> <ul style="list-style-type: none"> <li><b>CN=Switch-Managers,CN=Users,DC=arubasecurity,DC=net</b></li> </ul>
<b>Enforcement Profiles</b>	
Profile Names	<p>Choose the enforcement profile that will be applied when members of the Active Directory group listed above are matched. For example:</p> <ul style="list-style-type: none"> <li><b>ArubaOS Switch-Manager</b>.</li> </ul>

- Click **Save**.

You return to the **Add Enforcement Policies > Rules** page, where the new enforcement rules are displayed:

**Figure 176 ArubaOS Switch- Manager and ViewOnly Enforcement Policy Rules**

The screenshot shows the 'Enforcement Policies' page under 'Configuration > Enforcement > Policies > Add'. There are three tabs: 'Enforcement', 'Rules' (which is selected), and 'Summary'. Under 'Rules Evaluation Algorithm', the 'Select first match' option is checked. The 'Enforcement Policy Rules' section contains two entries:

Conditions	Actions
1. (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-Managers,CN=Users,DC=arubasecurity,dc=net) 2. (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-ViewOnly,CN=Users,DC=arubasecurity,DC=net)	[RADIUS] ArubaOS-Switch-Manager [RADIUS] ArubaOS-Switch-ViewOnly

Buttons at the bottom include 'Add Rule', 'Move Up', 'Move Down', 'Edit Rule', 'Remove Rule', 'Back to Enforcement Policies', 'Next >', 'Save', and 'Cancel'.

- Click **Next**.

The **Add Enforcement Policies > Summary** page opens:

**Figure 177 ArubaOS RADIUS Enforcement Policy Summary**

The screenshot shows the 'Enforcement Policies' page under 'Configuration > Enforcement > Policies > Add'. The 'Summary' tab is selected. A message 'Enforcement policy has not been saved' is displayed. The 'Enforcement:' section includes:

Name:	ArubaOS-Switch-RADIUS-Policy
Description:	Enforcement policy for ArubaOS-Switch
Enforcement Type:	RADIUS
Default Profile:	[Deny Access Profile]

The 'Rules:' section shows the same two rules as in Figure 176:

Conditions	Actions
1. (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-Managers,CN=Users,DC=arubasecurity,dc=net) 2. (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-ViewOnly,CN=Users,DC=arubasecurity,DC=net)	[RADIUS] ArubaOS-Switch-Manager [RADIUS] ArubaOS-Switch-ViewOnly

Buttons at the bottom include 'Back to Enforcement Policies', 'Next >', 'Save', and 'Cancel'.

- Repeat Step 4 through Step 7 for each role you need to add to the enforcement policy (such as *ViewOnly*), with the only differences being the **memberOf** value and **Enforcement Profile** value.
- Click **Save**.

You return to the **Enforcement Policies** page where the following message is displayed:

*Enforcement policy "ArubaOS-Switch-RADIUS-Policy" has been added.*

## Setting Up a Service in ClearPass to Support RADIUS Authentication Requests From the Switch

The service to support RADIUS authentication requests from the ArubaOS switch incorporates the previously-created elements:

- Enforcement profiles that define manager-level access and operator-level access to the ArubaOS switch (see [Creating Enforcement Profiles to Provide Manager Access and Command Authorization to the ArubaOS Switch on page 216](#)).
- Enforcement policy that defines access to the ArubaOS switch (see [Creating an Enforcement Policy to Define Access to the Switch on page 221](#)).

To create a service to authenticate RADIUS users against Active Directory:

- Navigate to **Configuration > Services**.
- From the **Services** page, click the **Add** link.

The **Add Configuration Services** page opens.

**Figure 178 Adding a RADIUS Enforcement Service**

Configuration > Services > Add Services

**Service** **Authentication** **Roles** **Enforcement** **Summary**

Type: RADIUS Enforcement ( Generic )

Name: ArubaOS-Switch-RADIUS

Description: Service to authenticate ArubaOS-Switch administrative users

Monitor Mode:  Enable to monitor network access without enforcement

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

**Service Rule**

Matches  ANY or  ALL of the following conditions:

Type	Name	Operator	Value
1. Connection	Protocol	EQUALS	RADIUS
2. Radius:IETF	Service-Type	EQUALS	NAS-Prompt-User (7)
3. Radius:IETF	NAS-Port-Type	EQUALS	Virtual (5)
4. Click to add...			

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

- Specify the **Add RADIUS Enforcement Service** parameters as described in the following table:

**Table 62: Add RADIUS Enforcement Service Parameters**

Parameter	Action/Description
Type	Select <b>RADIUS Enforcement (Generic)</b> .
Name	Enter a name for this service.
Description	Optionally (but recommended), add a description of this enforcement service.
Monitor Mode	This option is disabled by default. Do not enable Monitor Mode.
More Options	No additional options are required for this service.
<b>Service Rule</b>	
Matches	Select <b>ALL of the following conditions</b> .

Parameter	Action/Description
<i>Rule condition 1:</i> Specifying the RADIUS protocol	Select <b>Click to add</b> , then specify the following attributes: <ul style="list-style-type: none"> <li>• Type: <b>Connection</b></li> <li>• Name: <b>Protocol</b></li> <li>• Operator: <b>EQUALS</b></li> <li>• Value: <b>RADIUS</b></li> </ul>
<i>Rule condition 2:</i> Specifying the Service-Type	Select <b>Click to add</b> , then specify the following attributes: <ul style="list-style-type: none"> <li>• Type: <b>Radius:IETF</b></li> <li>• Name: <b>Service-Type</b></li> <li>• Operator: <b>EQUALS</b></li> <li>• Value: <b>NAS-Prompt-User</b></li> </ul>
<i>Rule condition 3:</i> Specifying the NAS-Port-Type	Select <b>Click to add</b> , then specify the following attributes: <ul style="list-style-type: none"> <li>• Type: <b>Radius:IETF</b></li> <li>• Name: <b>NAS-Port-Type</b></li> <li>• Operator: <b>EQUALS</b></li> <li>• Value: <b>Virtual</b></li> </ul>

4. Click **Next**.

The **Authentication** tab opens.

**Figure 179 RADIUS Enforcement Service > Authentication Tab**

The screenshot shows the 'Add Services' configuration page. The 'Authentication' tab is active. In the 'Authentication Methods' section, '[PAP]' is listed in a dropdown menu with options: Move Up, Move Down, Remove, View Details, and Modify. In the 'Authentication Sources' section, 'Aruba Security AD [Active Directory]' is listed in a dropdown menu with the same set of options. Other sections include 'Strip Username Rules' (checkbox) and 'Service Certificate' (dropdown). At the bottom, there are 'Back to Services', 'Next >', 'Save', and 'Cancel' buttons.

5. From the **Authentication Sources** drop-down, select **Aruba Security AD** (or whatever name was assigned to this authentication source).
6. Select the **Enforcement** tab.

**Figure 180 RADIUS Enforcement Service > Enforcement Tab**

Enforcement Policy Details		Enforcement Profiles
Description:	Enforcement policy for ArubaOS-Switch	
Default Profile:	[Deny Access Profile]	
Rules Evaluation Algorithm:	first-applicable	
Conditions		
1. (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-Managers,CN=Users,DC=arubasecurity,dc=net)	ArubaOS-Switch-Manager	
2. (Authorization:Aruba Security AD:memberOf EQUALS CN=Switch-ViewOnly,CN=Users,DC=arubasecurity,DC=net)	ArubaOS-Switch-ViewOnly	

7. From the **Enforcement Policy** drop-down, select **ArubaOS-Switch-RADIUS-Policy**.

8. Click **Save**.

This completes the service for ArubaOS switch management.

## OnGuard Authentication Configuration

This section contains the following information:

- [Overview](#)
- [OnGuard Configuration Workflow](#)
- [OnGuard Authentication Configuration](#)
- [ClearPass Configuration](#)

### Overview

This section describes a basic OnGuard deployment using the persistent agent to provide posture checks on centrally managed Windows devices that are connected via Ethernet to an ArubaOS switch.

- For detailed information about the OnGuard health checks for Windows, macOS, and Linux, refer to "Configuring Posture Policy Agents and Hosts" in Chapter 6, "Posture Policies and Audit Servers" in the *ClearPass 6.7 Policy Manager User Guide*.

Policy Manager provides several methods for assessing the health posture of clients requesting access: OnGuard Agents, NAP Agents, and NESSUS or NMAP scans. All of these methods return posture tokens (for example, *Healthy*, *Quarantine*) that Policy Manager uses to provide input into enforcement policies.

One or more of these posture methods can be associated with a service. ClearPass OnGuard performs advanced endpoint posture assessments by running checks on the endpoints that are attempting to gain access to the network.

You can use information provided by the OnGuard agent about endpoint integrity (such as status of anti-virus, firewall, and peer-to-peer applications) to enhance authorization policies. Automatic remediation services are also available for noncompliant devices.

### OnGuard Agent

The OnGuard Agent enables more extensive health checks than those available in the NAP Agent. Both persistent and dissolvable agents are available for Windows, macOS, and Linux operating systems.

- The *persistent agent* is installed on the end system and runs in the background. It requires network connectivity. The persistent agent regularly reports health information to a ClearPass Webauth posture check service.
- The *dissolvable agent* does not permanently install anything on the end system. The user is redirected to the ClearPass Web Login page created by the administrator. The OnGuard agent is run on-demand in the web browser.

## Posture Policy Checks

Both the persistent and dissolvable agents cache the health results in the Endpoint Database. The latest health posture token can be used by ClearPass services. The persistent and dissolvable agents perform the same health checks, but auto-remediation is only available with the persistent agent.

Depending on the operating system where OnGuard is installed, there are multiple health checks that can be performed by the OnGuard agent. Some health checks are not applicable on all operating systems.

For example, when the macOS operating system is selected, the available health checks do not include "Windows Hotfixes" or "Registry Keys" as possible checks for OnGuard to perform.

## OnGuard Configuration Workflow

The following ClearPass components must be configured to configure OnGuard:

1. Define the posture policy (see [Defining the Posture Policy](#) below).
2. ClearPass Configuration
  - Agent settings
  - Policy Manager Zone mapping
  - Policy Manager service
  - ClearPass Web Authorization page
3. ArubaOS switch configuration

## ClearPass Configuration

This section describes the ClearPass configuration required for configuring OnGuard authentication. The major ClearPass configuration tasks are as follows:

- [OnGuard Authentication Configuration](#)
- [Defining Policy Manager Zones](#)
- [Configuring OnGuard Settings](#)
- [Configuring Posture Policies](#)
- [OnGuard Authentication Configuration](#)
- [OnGuard Authentication Configuration](#)

## Defining the Posture Policy

Before you configure the posture policy, determine the following elements:

- Which end systems the OnGuard agents will be installed on
- What health checks need to be performed on the end system(s)
- What results will be required to return a Healthy Token

These decisions will be the basis for the ClearPass posture policy that you will configure later in this chapter (see [Configuring Posture Policies](#)).

## Defining Policy Manager Zones

To define the Policy Manager Zones:

ClearPass Policy Managershares 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 information to a given geographical area.

You can configure zones in ClearPass to match the geographical areas in your deployment. There can be multiple zones per cluster, and each zone has a number of ClearPass nodes that share their run-time state.

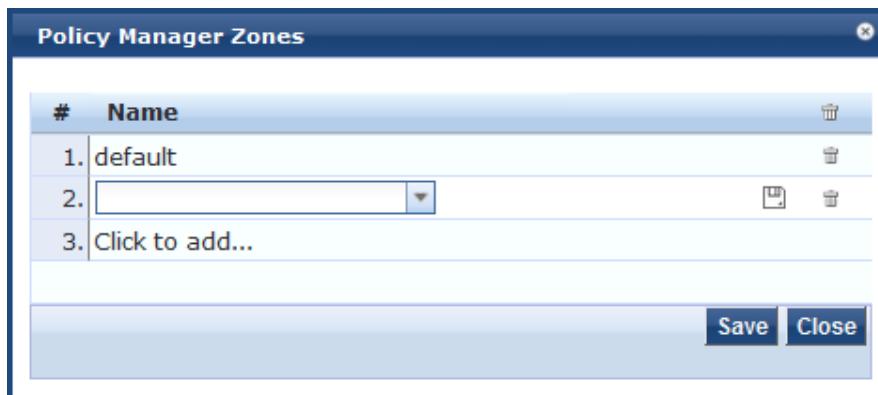
### Adding Policy Manager Zones

To add a ClearPass 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:

**Figure 181** *Policy Manager Zones Dialog*



3. To add a new ClearPass Policy Manager Zone, click **Click to add...** and enter the name of the ClearPass 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 (>Delete).

### Mapping Policy Manager Zones to OnGuard Clients

To configure the ClearPass 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 182** *Mappings for ClearPass Policy Manager Zones to OnGuard Clients Page*

#	Policy Manager Zone	Client Subnets	Server IPs
No Policy Manager Zone settings configured			

**Zone Network Details -**

Policy Manager Zone:	West_Coast
Client Subnets (e.g., 192.168.1.1/24):	192.0.2.0/24
Default ClearPass Server IPs:	Not assigned
Override Server IPs (optional):	

**Buttons:** Reset, Delete, Save, Close

3. Specify the **Mappings for ClearPass Policy Manager Zones to OnGuard Clients** parameters as described in the following table:

**Table 63:** *OnGuard Settings > Zones Parameters*

Parameter	Action/Description
ClearPass Policy Manager Zone	Select the ClearPass Policy Manager Zone from the drop-down list. If no ClearPass Policy Manager zone is configured, the default ClearPass Policy Manager zone is displayed in this field.
Client Subnets	Displays the client subnet addresses specified for the selected ClearPass Policy Manager zone.
Server IPs	Displays the server IP addresses specific to the selected ClearPass Policy Manager zone.
<b>Zone Network Details</b>	
ClearPass Policy Manager Zone	Select the ClearPass Policy Manager zone from the drop-down list that is created from the <b>Administration &gt; Server Manager &gt; Server Configuration &gt; Manage Policy Manager Zones</b> page.

Parameter	Action/Description
Client Subnets	Specify the client subnets that are configured for the selected zone.
Default ClearPass Server IPs	Specify the IP address of the default ClearPass Policy Manager server.
Override Server IPs	<p>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.</p> <p>You can specify the data port or load balancer IP address in this field.</p> <p>The IP addresses configured here will override the IP address configured in the <b>Default ClearPass Server IPs</b> field.</p> <p>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.</p>

## Configuring OnGuard Settings

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 hardware or virtual appliance.

You can then publish this URL to the user community or download the agent deployment packages to another location.

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 183** *OnGuard Settings Page > Settings Tab*

Administration » Agents and Software Updates » OnGuard Settings -

OnGuard Settings -

**Settings** **Installers**

Agent Version: 6.7.4.106664

Agent Library Version: 1.0.4.106664

Installer Mode: Do not install/enable Aruba VIA component

Agent will be used only to authenticate/perform health checks for client machines. This setting will not install the Aruba VIA component. If already installed, then the VIA component will be disabled on the client machine.

**Note: This WILL remove any existing/installed Aruba VIA client**

**Agent Customization**

Managed Interfaces:  Wired  Wireless  VPN  Other

Mode: Authenticate with health checks

Username Text:  Username

Password Text:  Password

Agent action when an update is available: Ignore

**Agent Remediation User Interface Customization**

Custom User Interface:  Configure

**Native Dissolvable Agent Customization**

Managed Interfaces:  Wired  Wireless  VPN  Other

2. Configure the **OnGuard Settings** parameters as described in the following table, then click **Save**.

**Table 64: OnGuard Settings Parameters**

Parameter	Action/Description
Global Agent Settings	Click the <b>Global Agent Settings</b> link to configure the global agent settings for OnGuard agents.
ClearPass Policy Manager Zones	Click the <b>Policy Manager Zones</b> link to configure the client subnets that comprise the ClearPass Policy Manager Zone.
Agent Version	Indicates the current version of the OnGuard agent.
Agent Library Version	Indicates the version of the OnGuard Agent Library. OnGuard Agent uses this library for health collection and auto-remediation.
Installer Mode	<p>Specify the action to be taken from the following options when the ClearPass VIA component is used to provide VPN-based access:</p> <ul style="list-style-type: none"><li>● <b>Do not install/enable Aruba VIA component</b> <b>NOTE:</b> Selecting this option will automatically remove any existing and installed ClearPass VIA client software.</li><li>● <b>Install and enable Aruba VIA component</b> <b>NOTE:</b> Selecting this option will automatically upgrade any existing and installed ClearPass VIA client software.</li></ul>
<b>Agent Customization</b>	
Managed Interfaces	Select the type(s) of interfaces that OnGuard will manage on the endpoint. Select from the following options: <ul style="list-style-type: none"><li>● <b>Wired</b></li><li>● <b>Wireless</b></li><li>● <b>VPN</b></li><li>● <b>Other</b></li></ul>
Mode	Select one of the following options: <ul style="list-style-type: none"><li>● <b>Authenticate with health checks:</b> OnGuard collects the username and password and also performs health checks on the endpoint. This is the default setting.</li><li>● <b>Authenticate - no health checks:</b> OnGuard collects username and password but does not perform health checks on the endpoint.</li><li>● <b>Check health - no authentication:</b> OnGuard does not collect the username and password.</li><li>● <b>Username/Password Text:</b> The label for the <i>Username</i> and <i>Password</i> fields on the OnGuard agent user interface.</li></ul>

Parameter	Action/Description
	<b>NOTE:</b> This setting is not valid for the <b>Check health - no authentication</b> mode.
Username Text	The label for the <i>Username</i> field on the OnGuard agent. This setting is not valid for the <b>Check health - no authentication</b> mode.
Password Text	The label for the <i>Password</i> field on the OnGuard agent. This setting is not valid for the <b>Check health - no authentication</b> mode.
Agent action when an update is available	<p>Determines what the ClearPass OnGuard Agent does when an update of OnGuard Agent Library is available. Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Ignore:</b> ClearPass OnGuard Agent ignores the available OnGuard Agent Library update.</li> <li>• <b>Notify User:</b> ClearPass OnGuard Agent notifies the user that a new version of the OnGuard Agent Library is available on the ClearPass server.</li> <li>• <b>Download and Install:</b> 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.</li> </ul>
<b>Agent Remediation User Interface Customization</b>	
Custom User Interface	<p>When you select the <b>Configure</b> check box, the <b>Agent Remediation User Interface Customization</b> dialog opens.</p> <ul style="list-style-type: none"> <li>• <b>Web Pages:</b> To create the OnGuard custom web pages and define the properties for the web pages, click the <b>Create</b> link for the corresponding web page.</li> </ul>
<b>Native Dissolvable Agent Customization</b>	
Managed Interfaces	<p>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.</p> <p>Select the type(s) of managed interfaces that are supported for the Native Dissolvable Agent. Select from the following options:</p> <ul style="list-style-type: none"> <li>• <b>Wired</b></li> <li>• <b>Wireless</b></li> <li>• <b>VPN</b></li> <li>• <b>Other</b></li> </ul>

## Configuring Posture Policies

Posture policies can be associated with ClearPass services to verify the security posture of end systems prior to granting network access. The policy defines the end-system operating system and the type of agent to deploy. The posture policy also tells the OnGuard agent which health checks to perform and defines the rules that determine what is required to return a Healthy Token to the ClearPass service.

For Windows end systems, the Microsoft NAP (Network Access Protection) agent and the OnGuard agent are both available. For Linux and macOS, only the OnGuard agent is available.

From the **Posture Policies** page, you can create a new posture policy or edit an existing policy.

To create a new posture policy:

1. Navigate to **Configuration > Posture > Posture Policies**.

The **Posture Policies** page opens.

2. Click the **Add** link.

The **Add Posture Policies** configuration dialog opens.

**Figure 184** Adding a Posture Policy for Windows

The screenshot shows the 'Posture Policies' configuration dialog. The 'Policy' tab is selected. The 'Policy Name' field contains 'Employee Posture Policy for Windows'. The 'Description' field contains 'Posture policy for employees using Microsoft Windows'. Under 'Posture Agent', 'OnGuard Agent (Persistent or Dissolvable)' is selected. Under 'Host Operating System', 'Windows' is selected. The 'Plugin Version' is set to 2.0. In the 'Restrict by Roles' section, 'Employee' is listed in the dropdown, and there is a 'Remove' button. At the bottom, there are buttons for 'Back to Posture Policies', 'Next →', 'Save', and 'Cancel'.

3. For detailed information about configuring posture policies, agents, and hosts, refer to Chapter 6, "Posture Policies and Audit Servers" in the *ClearPass 6.7 Policy Manager User Guide*.

### Restricting Policies

The **Restrict by Roles** section of the **Policy** tab allows the administrator to apply the posture policy only to end systems that authenticate with selected roles. Typically users with access to sensitive information would authenticate with roles associated with more restrictive posture policies.

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 information, customer personal information, or health data could configure a posture policy that requires full disk encryption.

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.

## Monitoring and Troubleshooting

This section contains the following information:

- [Monitoring Active 802.1X Sessions](#)
- [Monitoring RADIUS Messages](#)

## Monitoring Active 802.1X Sessions

You can examine any active 802.1X sessions, and capture the users' Domain/User ID and the MAC address of the endpoint.

To monitor active 802.1X sessions:

```
ArubaOS-switch# show port-access authenticator clients
```

This command displays the following information:

- Port
- Client name
- MAC address
- IP address
- Client status

## Monitoring RADIUS Messages

To monitor the RADIUS messages between the switch and the ClearPass server, use the following command:

```
ArubaOS-switch# show radius authentication
```

**Figure 185** Monitoring Overview of Activity Between the NAS and the ClearPass Server

Status and Counters - RADIUS Authentication Information						
NAS Identifier						
Invalid Server Addresses	:	0				
UDP						
Server IP Addr	Port	Timeouts	Requests	Challenges	Accepts	Rejects
-----	-----	-----	-----	-----	-----	-----
10. [REDACTED]	1812	4	2000	1457	542	1
10. [REDACTED]	1812	0	0	0	0	0

## Using the show radius host Command

For a more detailed view of the interaction between the NAS and ClearPass, the **show radius host** command provides insight into the activity at the RADIUS level.

```
ArubaOS-switch# show radius host 10.x.x.x
```

**Figure 186** Monitoring Details of Activity Between the Switch and the ClearPass Server

Status and Counters - RADIUS Server Information	
Server IP Addr : 10.	
Authentication UDP Port	: 1812
Round Trip Time	: 4
Pending Requests	: 0
Retransmissions	: 4
Timeouts	: 4
Malformed Responses	: 0
Bad Authenticators	: 0
Unknown Types	: 0
Packets Dropped	: 0
Access Requests	: 2024
Access Challenges	: 1475
Access Accepts	: 548
Access Rejects	: 1
Accounting UDP Port	: 1813
Round Trip Time	: 0
Pending Requests	: 0
Retransmissions	: 1
Timeouts	: 1
Malformed Responses	: 0
Bad Authenticators	: 0
Unknown Types	: 0
Packets Dropped	: 0
Accounting Requests	: 3058
Accounting Responses	: 3058

As shown in [Figure 186](#), the break-out of port message information by **Authentication UDP Port** and **Accounting UDP Port** is of particular interest.



This chapter includes the following information:

- [Introduction](#)
- [Cisco Switch Configuration for ClearPass](#)
- [802.1X Service Setup](#)
- [Cisco Downloadable ACL \(dACL\) Setup](#)
- 

### Introduction

This chapter provides the set-up instructions for integrating a Cisco switch with ClearPass Policy Manager. This includes 802.1x, MAC address, and downloadable Access Control List (dACL) authentications.

### Assumptions

Basic familiarity with most Cisco switches is assumed.

For in-depth information about the features and functions of ClearPass, refer to the *ClearPass 6.7 User Guide*.

Cisco switches support multiple authentication methods and many RADIUS options that are passed to the switch. This chapter discusses only the subset of Cisco switch configuration features that are required for integration with ClearPass.

### Requirements

- Cisco LAN switch that supports 802.1X and MAC Authentication Bypass
- DHCP server for the registration VLAN and the mandatory VLANs (see [VLAN Numbers on page 239](#))
- Current ClearPass 6.7 Policy Manager release
- Verify that a basic configuration of ClearPass has been completed, which consists at minimum of initial set up and configuring a generic RADIUS service.

### Save Each Configuration Change

After each configuration change, exit the configure terminal mode and perform a **write memory** command to save the configuration.

## Cisco Switch Configuration for ClearPass

This section provides the following information:

- [Introduction](#)
- [VLAN Numbers](#)
- [Configuring the Cisco Switch](#)
- [Supplemental Configuration Information](#)

## Introduction

It is assumed that VLAN1 has been created for the Cisco switch with a correlating network-accessible IP address.

This network-accessible IP address must be able to communicate with the ClearPass Policy Manager server Data IP address.

If a single IP address is configured in the ClearPass server, the switch network-accessible IP address must be able to communicate with the ClearPass Management IP address.

## VLAN Numbers

The following VLAN numbers are used in the Cisco switch configuration:

**Table 65: VLAN Numbers**

Port	Description
999	Users and access points <b>NOTE:</b> In some circumstances, it may be necessary to set the default VLAN to 999.
333	Untrusted devices <b>NOTE:</b> If the ClearPass server goes offline, all users gain access to VLAN 333.
200	VoIP phones
60	Printers
50	Security network

## Configuring the Cisco Switch

To configure the Cisco switch:

1. Log into the Cisco switch.
2. Verify that the Cisco switch can ping the ClearPass server:

```
Cisco-switch# ping 192.0.2.10
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
```

3. In the event an error is received, verify the following:
  - a. The correct IP address for the default-gateway is set.
  - b. The firewall is not blocking the switch-to-ClearPass server communication.
4. Enable the new access control commands and functions to include advanced features using the following command:

```
Cisco-switch#config t
```

```
Cisco-switch(config)# aaa new-model
```

5. Add the ClearPass server as the RADIUS server with the following commands:

```
Cisco-switch(config)# radius-server host 192.0.2.10
```

```
Cisco-switch(config-radius-server)# address ipv4 192.0.2.10
```

```
Cisco-switch(config-radius-server)# key aruba123
```

```
Cisco-switch(config-radius-server) # exit  
Cisco-switch(config) #
```

6. Run the following command to enable 802.1x:

```
Cisco-switch(config) # dot1x system-auth-control
```

7. Use the following commands to set the switch to use RADIUS for AAA Authentication and Accounting:

```
Cisco-switch(config) # aaa authentication dot1x default group radius  
Cisco-switch(config) # aaa authorization network default group radius  
Cisco-switch(config) # aaa accounting dot1x default start-stop group radius
```

8. Add an AAA server for dynamic authorization:

```
Cisco-switch(config) # aaa server radius dynamic-author  
Cisco-switch(config-locsvr-da-radius) # client 192.0.2.10 server-key aruba123  
Cisco-switch(config-locsvr-da-radius) # port 3799  
Cisco-switch(config-locsvr-da-radius) # auth-type all  
Cisco-switch(config-locsvr-da-radius) # exit  
Cisco-switch(config) #
```

9. Use best practices to create standardized naming conventions that describe VLAN purposes and locations (refer to [Table 65](#)).

```
Cisco-switch(config) # vlan 999  
Cisco-switch(config-vlan) # name "Users and APs"  
Cisco-switch(config-vlan) # exit  
Cisco-switch(config) # vlan 333  
Cisco-switch(config-vlan) # name "Untrusted Devices"  
Cisco-switch(config-vlan) # exit  
Cisco-switch(config) # vlan 200  
Cisco-switch(config-vlan) # name "VoIP Phones"  
Cisco-switch(config-vlan) # exit  
Cisco-switch(config) # vlan 60  
Cisco-switch(config-vlan) # name "Printers"  
Cisco-switch(config-vlan) # exit  
Cisco-switch(config) # vlan 50  
Cisco-switch(config-vlan) # name "Security Network"  
Cisco-switch(config-vlan) # exit  
Cisco-switch(config) #
```



---

The Cisco switch is also the router.

---

10. Create interfaces on each VLAN.

If the Cisco switch is not acting as the router (or does not have Layer-3 capability), the VLANs and interface commands must be passed to the router.

The run commands are as follows:

```
Cisco-switch(config) #interface vlan 999  
Cisco-switch(config-if) # ip address 192.0.2.1 255.255.255.0  
Cisco-switch(config-if) # ip helper-address 192.0.2.10  
Cisco-switch(config-if) # ip helper-address 192.0.2.5  
Cisco-switch(config-if) # exit
```

```

Cisco-switch(config)#interface vlan 333
Cisco-switch(config-if)# ip address 192.168.33.1 255.255.255.0
Cisco-switch(config-if)# ip helper-address 192.0.2.10
Cisco-switch(config-if)# ip helper-address 192.0.33.5
Cisco-switch(config-if)# exit

Cisco-switch(config)#interface vlan 200
Cisco-switch(config-if)# ip address 192.168.200.1 255.255.255.0
Cisco-switch(config-if)# ip helper-address 192.0.2.10
Cisco-switch(config-if)# ip helper-address 192.0.200.5
Cisco-switch(config-if)# exit

Cisco-switch(config)#interface vlan 60
Cisco-switch(config-if)# ip address 192.168.60.1 255.255.255.0
Cisco-switch(config-if)# ip helper-address 192.0.2.10
Cisco-switch(config-if)# ip helper-address 192.0.2.5
Cisco-switch(config-if)# exit

Cisco-switch(config)#interface vlan 50
Cisco-switch(config-if)# ip address 192.168.50.1 255.255.255.0
Cisco-switch(config-if)# ip helper-address 192.0.2.10
Cisco-switch(config-if)# ip helper-address 192.0.2.5
Cisco-switch(config-if)# exit

```

## Supplemental Configuration Information

1. Verify the RADIUS server settings and applicable VLANs router interfaces for the VLANs that have been set prior to configuring a port to perform the 802.1x and MAC authentication bypass (also known as *MAC authentication fallback*).

 192.0.2.5 is the DHCP server and will vary based on the local configuration. 192.0.2.10 refers to the ClearPass Policy Manager server for the DHCP request in order for the device to be profiled.

2. Determine the interface type and numbering conventions using the **show interfaces description** command.  
The following list of interfaces (ports) will be displayed:
  - Fa = FastEthernet or 100 Mbps
  - Gi = GigabitEthernet or 1,000 Mbps
3. Use **Fa1/0/24**, which is the 24th copper port on the 3750 switch.
4. Use the following commands for port configuration:

 Interface type and numbering will differ from model to model.

```

Cisco-switch(config)# interface FastEthernet1/0/24
Cisco-switch(config-if)# switchport access vlan 333

```




---

This sets the port to access mode (untagged) with an untagged VLAN of 333 (the untrusted devices VLAN).

---

```
Cisco-switch(config-if)# switchport mode access
Cisco-switch(config-if)# authentication order dot1x mab
Cisco-switch(config-if)# authentication priority dot1x mab
Cisco-switch(config-if)# authentication port-control auto
Cisco-switch(config-if)# authentication periodic
Cisco-switch(config-if)# authentication timer reauthenticate server
Cisco-switch(config-if)# mab
```




---

MAC Authentication Bypass (MAB) permits the port to perform MAC authentication if the switch detects that the device is not 802.1x capable. MAB is enabled after 40 seconds.

---

```
Cisco-switch(config-if)# dot1x pae authenticator
Cisco-switch(config-if)# dot1x timeout server-timeout 30
Cisco-switch(config-if)# dot1x timeout tx-period 10
Cisco-switch(config-if)# dot1x timeout supp-timeout 30
Cisco-switch(config-if)# dot1x max-req 3
Cisco-switch(config-if)# dot1x max-reauth-req 10
Cisco-switch(config-if)# spanning-tree portfast
Cisco-switch(config-if)# exit
```

5. Run the following commands to ensure that Downloadable Access Control Lists (DACL) will work correctly:

```
Cisco-switch(config)# ip dhcp snooping
Cisco-switch(config)# ip device tracking
Cisco-switch(config)# radius-server vsa send authentication
```

## 802.1X Service Setup

This section provides the following information:

- [Introduction](#)
- [Adding an Enforcement Profile for VLAN 999](#)

### Introduction

Service setup requires a set of rules known as **enforcement profiles**. You can configure Policy Manager enforcement profiles globally, but they must be referenced to an enforcement policy that is associated with a service.

Each enforcement profile can have an associated group of Network Access Devices (NADs).

In the following procedure, you will configure two enforcement profiles—one enforcement profile will return VLAN 999 and one enforcement profile will return a Cisco downloadable ACL (dACL).

### Adding an Enforcement Profile for VLAN 999

To add the enforcement profile for VLAN 999:

1. Navigate to **Configuration > Enforcement > Profiles**.

The **Enforcement Profiles** page opens:

**Figure 187 Enforcement Profiles Page**

The screenshot shows a table titled "Enforcement Profiles" with the following data:

#	Name	Type	Description
1.	[Aerohive - Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aerohive)
2.	[AirGroup Personal Device]	RADIUS	System-defined profile for an AirGroup personal device request
3.	[AirGroup Response]	RADIUS	System-defined profile for any AirGroup request
4.	[AirGroup Shared Device]	RADIUS	System-defined profile for an AirGroup shared device request
5.	[Allow Access Profile]	RADIUS	System-defined profile to allow network access
6.	[Allow Application Access Profile]	Application	System-defined profile to allow access to application
7.	[Aruba Bounce Host-Port]	RADIUS_CoA	System-defined profile to bounce host-port (Aruba)
8.	[Aruba TACACS read-only Access]	TACACS	System-defined profile for read-only access to Aruba device
9.	[Aruba TACACS root Access]	TACACS	System-defined profile for root access to Aruba device
10.	[Aruba Terminate Session]	RADIUS_CoA	System-defined profile to disconnect user (Aruba)

Showing 1-10 of 34 ► | Copy | Export | Delete |

- Click **Add**.

The **Add Enforcement Profiles** dialog opens.

**Figure 188 Adding an 802.1X Enforcement Profile**

The screenshot shows the "Add Enforcement Profile" dialog with the "Profile" tab selected. The fields are as follows:

- Template:** VLAN Enforcement
- Name:** VLAN 999
- Description:** Users and APIs
- Type:** RADIUS
- Action:**  Accept  Reject  Drop
- Device Group List:** A dropdown menu with options: Remove, View Details, Modify, and --Select--. An "Add new Device Group" link is also present.

- Enter the following values in the **Add Enforcement Profile > Profile** dialog:

- Template:** Select **VLAN Enforcement**.
- Name:** Enter **VLAN 999**.
- Description:** Optionally enter a description of this profile (recommended).
- Action:** Accept the default value: **Accept**.

- Click **Next**.

The **Enforcement Profile > Attributes** dialog opens.

**Figure 189** Selecting the Enter VLAN Value

Configuration » Enforcement » Profiles » Add Enforcement Profile

### Enforcement Profiles

Type	Name	Value	
1. Radius:IETF	Session-Timeout	= 10800	
2. Radius:IETF	Termination-Action	= RADIUS-Request (1)	
3. Radius:IETF	Tunnel-Type	= VLAN (13)	
4. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)	
5. Radius:IETF	Tunnel-Private-Group-Id	= Enter VLAN	
6. Click to add...			

5. In the **Tunnel-Private-Group-ID** attribute, click **Enter VLAN**.

6. Enter the VLAN value **999**, then click **Save** (see [Figure 190](#)).

**Figure 190** Specifying the VLAN Number

Configuration » Enforcement » Profiles » Add Enforcement Profile

### Enforcement Profiles

Type	Name	Value	
1. Radius:IETF	Session-Timeout	= 10800	
2. Radius:IETF	Termination-Action	= RADIUS-Request (1)	
3. Radius:IETF	Tunnel-Type	= VLAN (13)	
4. Radius:IETF	Tunnel-Medium-Type	= IEEE-802 (6)	
5. Radius:IETF	Tunnel-Private-Group-Id	= 999	
6. Click to add...			

7. Click the **Save to Disk** icon.

8. To review the enforcement profile settings and display the **Profile Summary**, click **Next**.

9. Confirm that the **Tunnel-Private-Group-ID** attribute is set to **999**, then click **Save**.

## Cisco Downloadable ACL (dACL) Setup

This section provides the following information:

- [Introduction](#)
- [Adding a Cisco dACL Enforcement Profile](#)
- [Adding a dACL Enforcement Policy](#)
- [Creating the 802.1X Wired Service](#)

### Introduction

You can download ACLs and redirect URLs from a RADIUS server (that is, the ClearPass server) to the switch during 802.1X authentication or MAC authentication bypass of the host. You can also download ACLs during web authentication.

If no ACLs are downloaded during 802.1X authentication, the switch applies the static default ACL on the port to the host.

Beginning with Cisco IOS Release 12.2(55)SE, if there is no static ACL on a port, a dynamic auth-default-ACL is created, and policies are enforced before dACLs are downloaded and applied.

## Adding a Cisco dACL Enforcement Profile

To add a Cisco dACL Enforcement Profile:

1. Navigate to **Configuration > Enforcement > Profiles**.  
The **Enforcement Profiles** page opens (see [Figure 187](#)).
2. Click **Add**.  
The **Add Enforcement Profiles** page opens.

**Figure 191** Adding a dACL Enforcement Profile

The screenshot shows the 'Add Enforcement Profile' dialog. It has tabs for 'Profile', 'Attributes', and 'Summary'. The 'Profile' tab is selected. The 'Template' field is set to 'Cisco Downloadable ACL Enforcement'. The 'Name' field contains 'Cisco dACL'. The 'Description' field is empty. The 'Type' field is set to 'RADIUS'. The 'Action' field has 'Accept' selected. The 'Device Group List' section shows a dropdown menu with options: 'Remove', 'View Details', and 'Modify'. A placeholder 'Device Group List' is visible below the dropdown.

3. Enter the following values in the **Add Enforcement Profile > Profile** dialog:
  - a. **Template**: Select **Cisco Downloadable ACL Enforcement**.
  - b. **Name**: Enter **Cisco dACL**.
  - c. **Description**: Optionally enter a description of this profile (recommended).
  - d. **Action**: Accept the default value: **Accept**.
4. Click **Next**.  
The **Enforcement Profile > Attributes** dialog opens.

**Figure 192** Specifying dACL Profile Attributes Value

The screenshot shows the 'Enforcement Profile > Attributes' dialog. It has tabs for 'Profile', 'Attributes', and 'Summary'. The 'Attributes' tab is selected. A table lists attributes:

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

The value for the **Cisco-IP-Downloadable-ACL** attribute is auto-populated (**permit ip any any**).

5. Click **Next** to accept the default value.  
The **Enforcement Profiles > Summary** page opens.
6. Verify that the settings are correct, then click **Save**.

## Adding a dACL Enforcement Policy

To add an enforcement policy:

1. Navigate to **Configuration > Enforcement > Policies**.

The **Enforcement Policies** page opens.

**Figure 193 Enforcement Policies Page**

The screenshot shows the 'Enforcement Policies' page with a list of 8 policies. The columns are 'Name', 'Type', and 'Description'. The policies listed are:

#	Name	Type	Description
1.	[Admin Network Login Policy]	TACACS	Enforcement policy controlling access to Policy Manager Admin
2.	[AirGroup Enforcement Policy]	RADIUS	Enforcement policy controlling access for AirGroup devices
3.	[Aruba Device Access Policy]	TACACS	Enforcement policy controlling access to Aruba device
4.	[Guest Operator Logins]	Application	Enforcement policy controlling access to Guest application
5.	[Insight Operator Logins]	Application	Enforcement policy controlling access to Insight application
6.	[Sample Allow Access Policy]	RADIUS	Sample policy to allow network access
7.	[Sample Deny Access Policy]	RADIUS	Sample policy to deny network access
8.	SnmpEnforcePolicy	WEBAUTH	AgentlessEnforce

2. Click **Add**.

The **Add Enforcement Policies** page opens.

**Figure 194 Adding an Enforcement Policy**

The screenshot shows the 'Add Enforcement Policies' dialog on the 'Enforcement' tab. The fields filled in are:

- Name: **Wired-Enforcement-with-dACL**
- Description: (empty)
- Enforcement Type: **RADIUS** (radio button selected)
- Default Profile: **Cisco dACL** (selected from dropdown)

3. Enter the following values in the **Add Enforcement Policies > Enforcement** dialog:

- Name:** Enter **Wired-Enforcement-with-dACL**.
- Description:** Optionally enter a description of this profile (recommended).
- Enforcement Type:** Accept the default value: **RADIUS**.
- Default Profile:** From the drop-down, select **Cisco dACL**.

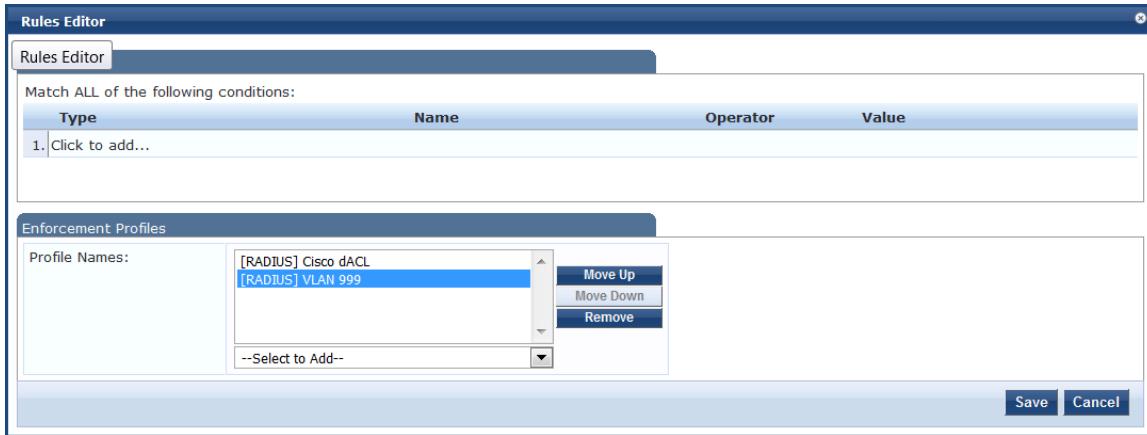
4. Click **Next**.

The **Enforcement Policies > Rules** dialog opens.

5. Click **Add Rule**.

The **Rules Editor** opens.

**Figure 195 Specifying Enforcement Policy Rules**



6. In the **Conditions** section, specify the following condition:
  - a. **Type:** Select **Date**.
  - b. **Name:** Select **Day-of-Week**.
  - c. **Operator:** Select **BELONGS\_TO**.
  - d. **Value:** Select **Monday, Tuesday, Wednesday, Thursday**.
7. In the Enforcement Profiles section, select the enforcement profiles associated with this policy.
  - a. **Profile Names:** From the **Select to Add** drop-down, select the following enforcement profiles that you created previously:
    - **[RADIUS] Cisco dACL**
    - **[RADIUS] VLAN 999**
8. Click **Save**, then click **Save** again.

## Creating the 802.1X Wired Service

Enforcement policies are always associated with a service, and a service can have only one policy associated with it.

To create the 802.1X wired service:

1. Navigate to **Configuration > Services**.  
The **Services** page opens.
2. Click **Add**.  
The **Add Services** page opens.

**Figure 196** Adding an 802.1X Wired Service

The screenshot shows the 'Services' configuration page with the 'Service' tab selected. A table lists service details:

Type:	802.1X Wired
Name:	Wired Enterprise Service
Description:	802.1X Wired Access Service
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Posture Compliance <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints <input type="checkbox"/> Accounting Proxy

**Service Rule**

Matches  ANY or  ALL of the following conditions:

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

3. Enter the following values in the **Add Services > Service** dialog:
  - a. **Type:** Select **802.1X Wired**.
  - b. **Name:** Enter **Wired Enterprise Service**.
  - c. **Description:** Enter **802.1X Wired Access Service**.
4. Click **Next**.

The **Add Services > Authentication** dialog opens.

**Figure 197** Specifying the Authentication Source

The screenshot shows the 'Authentication' tab of the 'Add Services > Authentication' dialog. It includes sections for 'Authentication Methods' and 'Authentication Sources'.

**Authentication Methods:** A list box contains [EAP PEAP], [EAP FAST], [EAP TLS], [EAP TTLS], and [EAP MSCHAPv2]. To the right is a context menu with options: Move Up, Move Down, Remove, View Details, and Modify.

**Authentication Sources:** A list box contains [Local User Repository] and [Local SQL DB]. The [Local User Repository] item is highlighted with a red border. To the right is a context menu with options: Move Up, Move Down, Remove, View Details, and Modify.

**Strip Username Rules:** A checkbox labeled 'Enable to specify a comma-separated list of rules to strip username prefixes or suffixes' is present.

5. From the **Authentication Sources** drop-down, select **[Local User Repository] [Local SQL DB]**.
6. Select the **Enforcement** tab.



# Mobility Access Switch Configuration for 802.1X Authentication

This chapter describes how to configure an Mobility Access Switch for 802.1X authentication.

This chapter includes the following information:

- [Mobility Access Switch Configuration for 802.1X Wired Authentication](#)
- [Configuring 802.1X Authentication with Machine Authentication](#)
- [CLI-Based Configuration for Mobility Access Switch 802.1X Authentication](#)

## Mobility Access Switch Configuration for 802.1X Wired Authentication

This section describes how to configure the Mobility Access Switch (MAS) for 802.1X wired authentication. This section contains the following information:

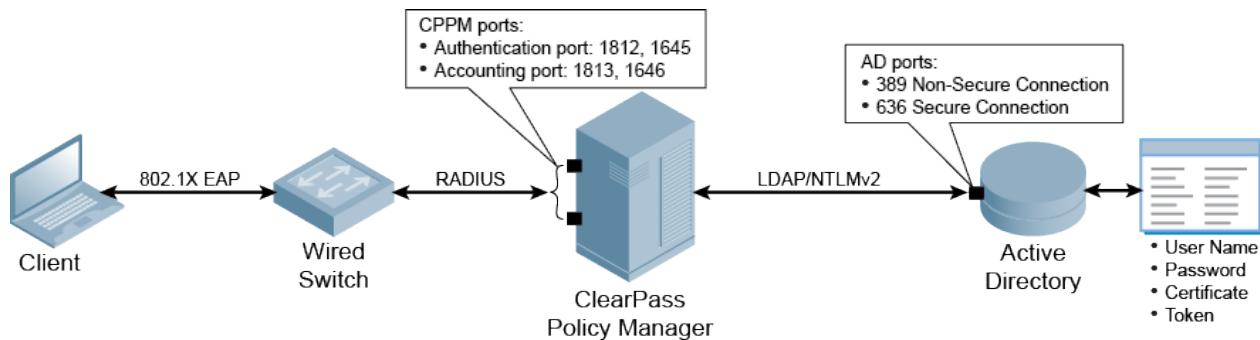
- [About Defining Wired 802.1X Authentication](#)
- [Configuring Authentication with a RADIUS Server](#)
- [Authentication Terminated on the Mobility Access Switch](#)
- [Configuring Access Control Lists](#)

### About Defining Wired 802.1X Authentication

Port-based 802.1X authentication on the Mobility Access Switch is configured similarly to how it's done on the mobility controller, the main difference being the AAA profile is applied on a wired interface or interface-group, as opposed to a Virtual Access Point (VAP) on the mobility controller.

[Figure 198](#) shows the network traffic flow for wired clients that connect to a Aruba Mobility Access Switch or a third-party switch and perform 802.1X authentication to the ClearPass Policy Manager server.

**Figure 198** Traffic flow for 802.1X Wired Authentication with Active Directory



The configuration process is as follows:

1. Define an external RADIUS server or create an internal database.
2. Define a server group and apply one of the servers above to this server group.
3. Create 802.1X authentication profiles.
4. Apply the server group to each of the 802.1X authentication profiles.
5. Apply the 802.1X authentication profiles to an AAA profile.

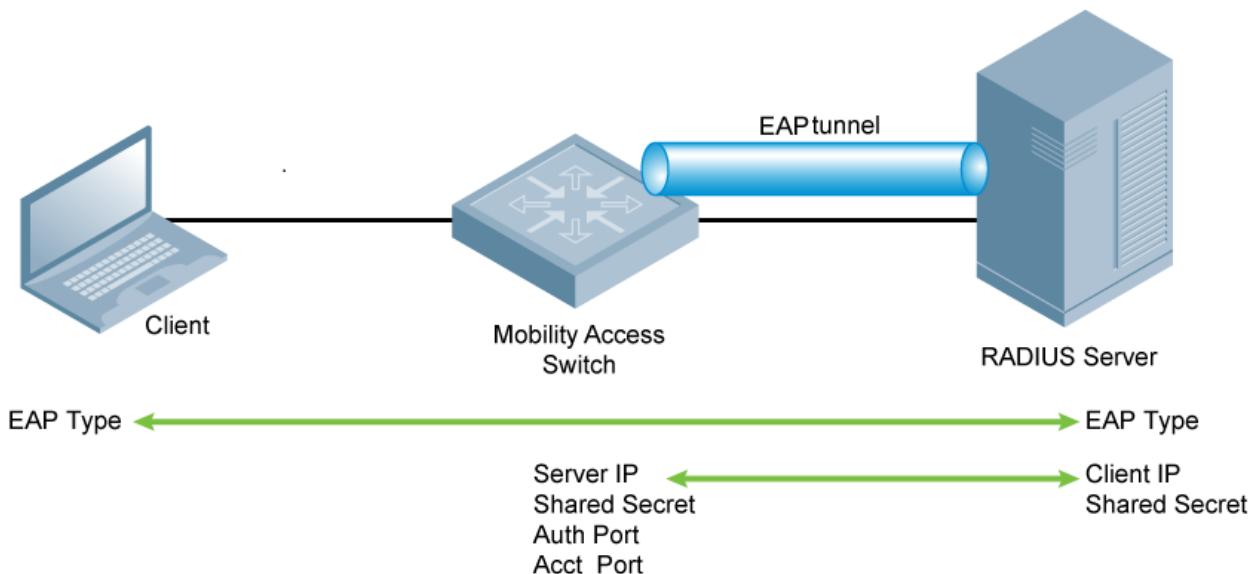
- Apply the AAA profile to the physical interface or interface group.

You can now configure an interface for 802.1X authentication.

## Configuring Authentication with a RADIUS Server

In order to authenticate to the network, the client communicates with the Mobility Access Switch through an EAP tunnel (see [Figure 199](#)). Therefore, the network authentication and encryption configured must be the same on both the client and the Mobility Access Switch.

**Figure 199** 802.1x Authentication with a RADIUS Server



To configure 802.1X authentication with a RADIUS server:

- For the Mobility Access Switch to communicate with the authentication server, you must configure the following parameters on the Mobility Access Switch:

Parameter	Action/Description
IP address	1. Enter the IP address of the authentication server.
Authentication port	2. Enter the Authentication port number on the authentication server. Default: <b>1812</b> .
Accounting port	3. Enter the Accounting port number on the authentication server. Default: <b>1813</b> .

- You must configure the supplicant (the client device) and authentication server (the Mobility Access Switch) to use the same EAP type.

The Mobility Access Switch doesn't need to know the EAP type used between the supplicant and authentication server.

- You must configure the authentication server with the IP address of the RADIUS client, which in this case is the Mobility Access Switch.
- Be sure to configure both the Mobility Access Switch and the authentication server to use the same shared secret.

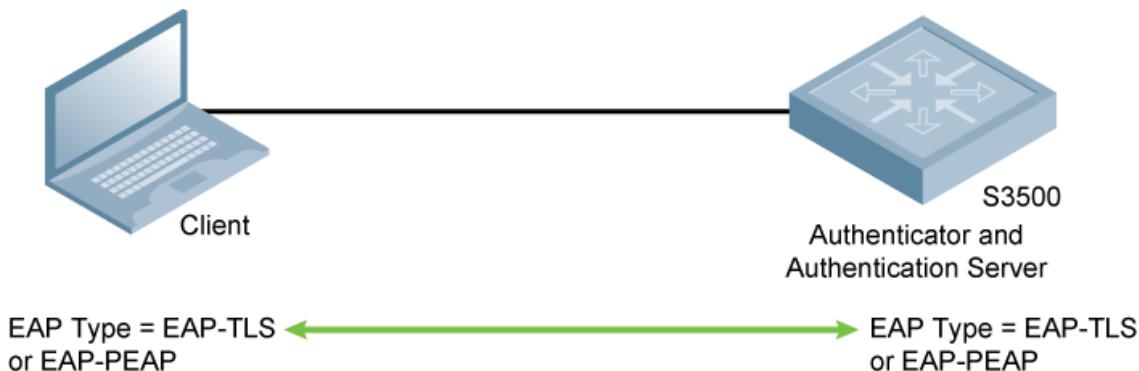


Additional information on EAP types supported in a Windows environment for Microsoft supplicants and the authentication server is available at [http://technet.microsoft.com/en-us/library/cc782851\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc782851(WS.10).aspx).

## Authentication Terminated on the Mobility Access Switch

User authentication is performed either via the Mobility Access Switch's internal database or a non-802.1x server.

**Figure 200** 802.1x Authentication with Termination on the Mobility Access Switch



In this scenario, the supplicant is configured for EAP-Protected EAP (PEAP) or EAP-Transport Layer Security (TLS).

### EAP-PEAP

EAP-PEAP uses TLS to create an encrypted tunnel. Within the tunnel, one of the following "inner EAP" methods is used:

- EAP-Generic Token Card (GTC)  
Described in RFC 2284, this EAP method permits the transfer of unencrypted usernames and passwords from client to server. The main uses for EAP-GTC are one-time token cards such as SecureID and the use of an LDAP or RADIUS server as the user authentication server.  
You can also enable caching of user credentials on the Mobility Access Switch as a backup to an external authentication server.
- EAP-Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2)  
Described in RFC 2759, this EAP method is widely supported by Microsoft clients. A RADIUS server must be used as the backend authentication server.

### EAP-TLS

EAP-TLS is used with smart-card user authentication. A smart card holds a digital certificate which, with the user-entered personal identification number (PIN), allows the user to be authenticated on the network. EAP-TLS relies on digital certificates to verify the identities of both the client and server.

EAP-TLS requires that you import server and certification authority (CA) certificates onto the Mobility Access Switch. The client certificate is verified on the Mobility Access Switch (the client certificate must be signed by a known CA) before the user name is checked on the authentication server.

### Internal Database Configuration Task

If you are using the Mobility Access Switch's internal database for user authentication, you need to add the names and passwords of the users to be authenticated.

## LDAP Server Configuration Task

If you are using an LDAP server for user authentication, you need to configure the LDAP server on the Mobility Access Switch, and configure user IDs and passwords.

## RADIUS Server Configuration Task

If you are using a RADIUS server for user authentication, you need to configure the RADIUS server on the Mobility Access Switch:

- For details, see [Configuring Authentication with a RADIUS Server on page 251](#).
- For the CLI example, see [Examples of Common 802.1X Configuration Tasks Via the CLI on page 261](#).

## Configuring Access Control Lists

To provide flexibility for controlling traffic, ArubaOS in Mobility Access Switches supports multiple types of Access Control Lists (ACLs).

- Ethertype ACL
  - Ethertype ACLs filter based on the *Ethertype* field in the frame header. Ethertype ACLs can be either named or numbered, with valid numbers in the range from 200 to 299. These ACLs can be used to permit IP, while blocking other non-IP protocols, such as IPX or AppleTalk.
- MAC ACL
  - MAC ACLs filter traffic on a specific source MAC address or range of MAC addresses. MAC ACLs can be either named or numbered, with valid numbers in the range from 700 to 799 and 1200 to 1299.
- Standard IP ACL
  - Standard ACLs permit or deny traffic based on the source IP address of the packet. Standard ACLs can be either named or numbered, with valid numbers in the range from 1 to 99 and 1300 to 1399. Standard ACLs use a bit-wise mask to specify the portion of the source IP address to be matched.
- Extended IP ACL
  - Extended ACLs permit or deny traffic based on the source or destination IP address, or the IP protocol. Extended ACLs can be named or numbered, with valid numbers in the range from 100 to 199 and 2000 to 2699.
- Stateless ACL
  - Stateless ACLs define stateless packet filtering and quality of service (QoS). A stateless ACL statically evaluates packet contents. The traffic in the reverse direction is allowed unconditionally.

Note that you can use names only when configuring stateless ACLs.

## Configuring a Stateless ACL

To configure a stateless ACL:

```
(ArubaSwitch) (config) #'''ip access-list stateless STATELESS'''  
(ArubaSwitch) (config-stateless-STATELESS) #'''any host 192.16.0.100 tcp 0 65535 permit'''
```

## Applying a Stateless ACL on a Physical Interface

To apply a stateless ACL on a physical interface:

```
(ArubaSwitch) (config) #'''interface gigabitethernet 0/0/8'''  
(ArubaSwitch) (gigabitethernet "0/0/8") #'''ip access-group in STATELESS'''
```

## Applying a Stateless ACL to a User Role

To apply a stateless ACL to a user role:

```
(ArubaSwitch) (config) #'''user-role EMPLOYEE_1'''  
(ArubaSwitch) (config-role) #'''access-list stateless STATELESS'''
```



You can also apply MAC and Ethertype ACLs to a user role. However, these ACLs apply only to a user's non-IP traffic.

## Verifiying Stateless ACL Configuration

To verify a stateless ACL configuration:

```
(ArubaSwitch) #'''show ip access-list STATELESS'''
```

## Verifying Stateless ACL Traffic Hits

To verify stateless traffic hits:

```
(ArubaSwitch) #'''show acl hits'''
```

## Verifying Stateless ACL Operation

To verify stateless ACL operation:

```
(ArubaSwitch) # '''show acl acl-table'''
```

# CLI-Based Configuration for Mobility Access Switch 802.1X Authentication

This section contains the following information:

- [Termination Options](#)
- [Configuring a Server Rule Using the CLI](#)
- [Setting Variables for LDAP Servers](#)
- [Configuring Certificates with Authentication Termination](#)

## Termination Options

The Mobility Access Switch supports 802.1x authentication, including *termination*. For example, the list of termination options for the profile name *FacultyAuth* is shown below.

```
(host) (802.1X Authentication Profile "FacultyAuth") # termination ?  
eap-type Configure the EAP method.Default method is EAP-PEAP  
enable Enable Dot1x Termination.Default is disabled  
enable-token-caching Enable Token Caching.Default is disabled  
inner-eap-type Configure the inner EAP method.Default method is  
EAP-MSCHAPV2  
token-caching-period Configure the Token Caching Period
```

## 802.1x Authentication Profile Configuration Examples

The following example configures various options for the 802.1x Authentication profile *FacultyAuth*.

```
(host) (802.1X Authentication Profile "FacultyAuth") #termination enable  
(host) (802.1X Authentication Profile "FacultyAuth") #termination eap-type eap-peap  
(host) (802.1X Authentication Profile "FacultyAuth") #max-authentication-failures 2  
(host) (802.1X Authentication Profile "FacultyAuth") #timer reauth-period 3600  
(host) (802.1X Authentication Profile "FacultyAuth") #framed-mtu 1500
```

```
(host) (802.1X Authentication Profile "FacultyAuth") #reauth-max 2  
(host) (802.1X Authentication Profile "FacultyAuth") #reauthentication
```

## Verifying Configurations

To verify the above configurations, execute the following **show** command:

```
(host) (config) #show aaa authentication dot1x FacultyAuth
```

Parameter	Value	
Max authentication failures	2	<--
Enforce Machine Authentication	Disabled	
Machine Authentication: Default Machine Role	guest	
Machine Authentication Cache Timeout	24 hr(s)	
Blacklist on Machine Authentication Failure	Disabled	
Machine Authentication: Default User Role	guest	
Interval between Identity Requests	30 sec	
Quiet Period after Failed Authentication	30 sec	
Reauthentication Interval	3600 sec	<--
Use Server provided Reauthentication Interval	Disabled	
Authentication Server Retry Interval	30 sec	
Authentication Server Retry Count	2	
Framed MTU	1500 bytes	<--
Number of times ID-Requests are retried	3	
Maximum Number of Reauthentication Attempts	2	<--
Maximum number of times Held State can be bypassed	0	
Reauthentication	Enabled	<--
Termination	Enabled	<--
Termination EAP-Type	eap-peap	<--
Termination Inner EAP-Type	N/A	
Enforce Suite-B 128 bit or more security level Authentication	Disabled	
Enforce Suite-B 192 bit security level Authentication	Disabled	
Token Caching	Disabled	
Token Caching Period	24 hr(s)	
CA-Certificate	N/A	
Server-Certificate	N/A	
TLS Guest Access	Disabled	
TLS Guest Role	guest	
Ignore EAPOL-START after authentication	Disabled	
Handle EAPOL-Logoff	Disabled	
Ignore EAP ID during negotiation.	Disabled	
Check certificate common name against AAA server	Enabled	



Use the privileged mode in the CLI to configure users in the Mobility Access Switch's internal database.

## Adding Users to the Local Database

To add users to the local database, use the following command:

```
local-userdb add username <user> password <password> role <user_role>
```

## Configuring a Server Rule Using the CLI

To configure a server rule using the CLI:

```
aaa server-group dot1x_internal  
set role condition Role value-of
```

## Setting Variables for LDAP Servers

If you are using a LDAP server for authentication, the following variables should be set:

- Termination enabled
- EAP type of PEAP (with inner-EAP-type set to **GTC**) or TLS

## LDAP Server Example Configuration

Below is an example configuration for the profile *FacultyAuth* for an LDAP server:

```
(host) (802.1X Authentication Profile "FacultyAuth") #termination enable  
(host) (802.1X Authentication Profile "FacultyAuth") #termination eap-type eap-peap  
(host) (802.1X Authentication Profile "FacultyAuth") # termination inner-eap-type eap-gtc
```

## Verifying the Configuration

To verify the configuration, execute the **show aaa authentication dot1x <profile\_name>** command.

## Configuring Certificates with Authentication Termination

The Mobility Access Switch supports 802.1x authentication using digital certificates for authentication termination.

- Server Certificate

A server certificate installed in the Mobility Access Switch verifies the authenticity of the Mobility Access Switch for 802.1x authentication. Mobility Access Switches ship with a demonstration digital certificate. Until you install a customer-specific server certificate in the Mobility Access Switch, this demonstration certificate is used by default for all secure HTTP connections and auth termination. This certificate is included primarily for feature demonstration and convenience and is not intended for long-term use in production networks.

Users in a production environment are urged to obtain and install a certificate issued for their site or domain by a well-known certificate authority (CA). You can generate a Certificate Signing Request (CSR) on the Mobility Access Switch to submit to a CA.

- Client Certificates

Client certificates are verified on the Mobility Access Switch (the client certificate must be signed by a known CA) before the user name is checked on the authentication server. To use client certificate authentication for auth termination you need to import the following certificates into the Mobility Access Switch:

- Mobility Access Switch's server certificate
- CA certificate for the CA that signed the client certificates

## Using the CLI

To use the CLI to configure certificates with authentication termination:

```
aaa authentication dot1x <profile>
    termination enable
    server-cert <certificate>
    ca-cert <certificate>
```

# Configuring 802.1X Authentication with Machine Authentication

This section contains the following information:

- [About Machine Authentication](#)
- [Enabling the Enforce Machine Authentication Option](#)
- [Role Assignment with Machine Authentication Enabled](#)
- [VLAN Assignments](#)
- [Authentication with an 802.1x RADIUS Server](#)
- [Examples of Common 802.1X Configuration Tasks Via the CLI](#)

## About Machine Authentication

When a Windows device boots, it logs onto the network domain using a machine account. Within the domain, the device is authenticated before computer group policies and software settings can be executed; this process is known as *machine authentication*. Machine authentication ensures that only authorized devices are allowed on the network.

## Enabling the Enforce Machine Authentication Option

You can configure 802.1X authentication for both user and machine authentication (for Windows environments only). This strengthens the authentication process further since both the device and user need to be authenticated.

Select the **Enforce Machine Authentication** option to enforce machine authentication before user authentication.

When selected, either **the Machine Authentication Default Role** or the **User Authentication Default Role** is assigned to the user, depending on which authentication is successful. This option is disabled by default.



This option may require a Policy Enforcement Firewall Next Generation (PEFNG) or Policy Enforcement Firewall Module (PEFV) license.

To enable **Enforce Machine Authentication**:

1. On the mobility controller, navigate to the **Configuration > SECURITY > Authentication > L2 Authentication** page.
2. In the Profiles list, expand the **802.1x Authentication** list and select the 802.1X Authentication profile of interest.  
The selected 802.1X Authentication Profile is displayed.

**Figure 201 Enabling the Enforce Machine Authentication Option**

The screenshot shows the 'Configuration' tab selected in the top navigation bar. Under 'Security > Authentication > L2 Authentication', the 'L2 Authentication' tab is active. On the left, a tree view lists profiles: MAC Authentication, 802.1X Authentication (with sub-options default, default-psk, default, dot1x\_prof-whn93, test), and Stateful 802.1X Authentication. The 'dot1x\_prof-whn93' profile is selected. The main panel displays the '802.1X Authentication Profile > dot1x\_prof-whn93' configuration. The 'Basic' tab is selected. In the 'Enforce Machine Authentication' row, there is a checked checkbox. Other settings include 'Max authentication failures' (0), 'Machine Authentication: Default Machine Role' (guest), 'Machine Authentication: Default User Role' (guest), 'Reauthentication' (unchecked), 'Termination' (unchecked), 'Termination EAP-Type' (eap-tls checked, eap-peap unchecked), 'Termination Inner EAP-Type' (eap-mschapv2 checked, eap-gtc unchecked), 'Enforce Suite-B 128 bit or more security level Authentication' (unchecked), and 'Enforce Suite-B 192 bit security level Authentication' (unchecked).

3. To enable the option, select the **Enforce Machine Authentication** check box.

## Role Assignment with Machine Authentication Enabled

When you enable machine authentication, there are two additional roles you can define in the 802.1x authentication profile:

- Machine authentication: default machine role
- Machine authentication: default user role

While you can select the same role for both options, you should define the roles according to the policies that need to be enforced. Also, these machine authentication roles can be different from the 802.1x authentication default role configured in the AAA profile.

With machine authentication enabled, the assigned role depends upon the success or failure of the machine and user authentications. In certain cases, the role that is ultimately assigned to a client can also depend upon attributes returned by the authentication server or server derivation rules configured on the Mobility Access Switch.

[Table 66](#) describes role assignment based on the results of the machine and user authentications.

**Table 66: Role Assignments for User and Machine Authentication**

Machine Auth Status	User Auth Status	Description	Role Assignment
Failed	Failed	Both machine authentication and user authentication failed. Layer 2 authentication failed.	Initial role defined in the AAA profile will be assigned. If no initial role is explicitly defined, the default initial role (logon role) is assigned.
Failed	Passed	Machine authentication fails (for example, the machine information is not present on the server) and user authentication succeeds. Server-derived roles do not apply.	Machine authentication default user role configured in the 802.1x authentication profile.
Passed	Failed	Machine authentication succeeds and user authentication has not been initiated. Server-derived roles do not apply.	Machine authentication default machine role configured in the 802.1x authentication profile.
Passed	Passed	Both machine and user are successfully authenticated. If there are server-derived roles, the role assigned via the derivation takes precedence. This is the <i>only</i> case where server-derived roles are applied.	A role derived from the authentication server takes precedence. Otherwise, the 802.1x authentication default role configured in the AAA profile is assigned.

### Role Assignments Example

For example, if the following roles are configured:

- 802.1x authentication default role (in AAA profile): **dot1x\_user**
- Machine authentication default machine role (in 802.1x authentication profile): **dot1x\_mc**
- Machine authentication default user role (in 802.1x authentication profile): **guest**

The Role assignments would be as follows:

- If both machine and user authentication succeed, the role is **dot1x\_user**. If there is a server-derived role, the server-derived role takes precedence.
- If only machine authentication succeeds, the role is **dot1x\_mc**.
- If only user authentication succeeds, the role is **guest**.
- On failure of both machine and user authentication, the initial role defined in the AAA profile is assigned.

### VLAN Assignments

With machine authentication enabled, the VLAN to which a client is assigned (and from which the client obtains its IP address) depends upon the success or failure of the machine and user authentications.

The VLAN that is ultimately assigned to a client can also depend upon attributes returned by the authentication server or server derivation rules configured on the Mobility Access Switch.

If machine authentication is successful, the client is associated to the VLAN configured on the interface. However, the client can be assigned a derived VLAN upon successful user authentication.



You can optionally assign a VLAN as part of a user role configuration. It is recommended not to use VLAN derivation if user roles are configured with VLAN assignments.

[Table 67](#) describes VLAN assignment based on the results of the machine and user authentications when VLAN derivation is used.

**Table 67: VLAN Assignments for User and Machine Authentication**

Machine Auth Status	User Auth Status	Description	VLAN Assignment
Failed	Failed	Both machine authentication and user authentication failed. Layer 2 authentication failed.	<ul style="list-style-type: none"><li>● VLAN configured on the interface.</li><li>● VLAN configured under initial role.</li></ul>
Failed	Passed	Machine authentication fails (for example, the machine information is not present on the server) and user authentication succeeds.	<ul style="list-style-type: none"><li>● VLAN configured on the interface.</li><li>● VLAN configured under machine authentication default user role.</li></ul>
Passed	Failed	Machine authentication succeeds and user authentication has not been initiated.	<ul style="list-style-type: none"><li>● VLAN configured on the interface.</li><li>● VLAN configured under machine authentication default user role.</li></ul>
Passed	Passed	Both machine and user are successfully authenticated.	<ul style="list-style-type: none"><li>● Derived VLAN.</li><li>● VLAN configured on the interface.</li></ul>

## Authentication with an 802.1x RADIUS Server

When authenticating with an 802.1X RADIUS server:

- An EAP-compliant RADIUS server provides the 802.1x authentication.  
The RADIUS server administrator must configure the server to support this authentication. The administrator must also configure the server to handle all communications with the Mobility Access Switch.
- 802.1x authentication based on PEAP with MS-CHAPv2 provides both computer and user authentication.  
If a user attempts to log in without the computer being authenticated first, the user is placed into a limited guest user role.  
Windows domain credentials are used for computer authentication, and the user's Windows login and password are used for user authentication. A single user sign-on facilitates both authentication to the network and access to the Windows server resources.

You can create the following policies and user roles for:

- Student
- Faculty

- Guest
- Sysadmin
- Computer

## Examples of Common 802.1X Configuration Tasks Via the CLI

This section provides several examples of common configuration tasks via the command line interface (CLI):

- [Creating an Alias for the Internal Network](#)
- [Creating the Student Role and Policy](#)
- [Creating the Faculty Role and Policy](#)
- [Creating the Guest Role and Policy](#)
- [Configuring the RADIUS Authentication Server](#)
- [Configuring 802.1x Authentication Profile](#)
- [Configuring the AAA Profile](#)

### Creating an Alias for the Internal Network

To create an alias for the internal network:

```
netdestination "Internal Network"
  network 10.0.0.0 255.0.0.0
  network 172.16.0.0 255.255.0.0
```

### Creating the Student Role and Policy

The *student* policy prevents students from using Telnet, POP3, FTP, SMTP, SNMP, or using SSH to access the wired portion of the network. The *student* policy is mapped to the *student* user role.

To create the Student role and policy:

```
ip access-list stateless student
  any alias "Internal Network" svc-telnet deny
  any alias "Internal Network" svc-pop3 deny
  any alias "Internal Network" svc-ftp deny
  any alias "Internal Network" svc-smtp deny
  any alias "Internal Network" svc-snmp deny
  any alias "Internal Network" svc-ssh deny
user-role student
access-list stateless student
access-list stateless allowall
```

### Creating the Faculty Role and Policy

The *faculty* policy is similar to the *student* policy. However, the faculty members are allowed to use POP3 and SMTP. The *faculty* policy is mapped to the *faculty* user role.

To create the Faculty role and policy:

```
ip access-list stateless faculty
  any alias "Internal Network" svc-telnet deny
  any alias "Internal Network" svc-ftp deny
  any alias "Internal Network" svc-snmp deny
  any alias "Internal Network" svc-ssh deny
user-role faculty
```

```
access-list stateless faculty
access-list stateless allowall
```

## Creating the Guest Role and Policy

The *guest* policy permits only access to the Internet (via HTTP or HTTPS) and only during daytime working hours. The *guest* policy is mapped to the *guest* user role.

To create the guest role and policy:

```
time-range working-hours periodic
    weekday 07:30 to 17:00
ip access-list stateless guest
    any host 10.1.1.25 svc-dhcp permit time-range working-hours
    any host 10.1.1.25 svc-dns permit time-range working-hours
    any alias "Internal Network" any deny
    any any svc-http permit time-range working-hours
    any any svc-https permit time-range working-hours
    any any any deny
user-role guest
access-list stateless guest
```

## Configuring the RADIUS Authentication Server

You can set the role condition to identify the user's group. The Mobility Access Switch uses the literal value of this attribute to determine the role name.

The following example uses the RADIUS server name *radiusFaculty* to configure the RADIUS server.

To configure the RADIUS authentication server to identify the user's group:

```
(host) (config) #aaa authentication-server radius radiusTechPubs
(host) (RADIUS Server "radiusFaculty") #host 10.41.255.30
(host) (RADIUS Server "radiusFaculty") #key hometown
(host) (RADIUS Server "radiusFaculty") #exit

(host) (config) #aaa server-group radiusTechpubs
(host) (Server Group "radiusFaculty") #auth-server radiusTechpubs
(host) (Server Group "radiusFaculty") #set role condition Class Value-of
```

## Configuring 802.1x Authentication Profile

In the 802.1x authentication profile, configure enforcement of machine authentication before user authentication (see [Enabling the Enforce Machine Authentication Option](#)).

If a user attempts to log in without machine authentication taking place first, the user is placed in the guest role.

To configure the 802.1X authentication profile:

```
aaa authentication dot1x dot1x
    machine-authentication enable
    machine-authentication machine-default-role student
    machine-authentication user-default-role guest
```

## Configuring the AAA Profile

An AAA profile specifies the 802.1x authentication profile and 802.1x server group to be used for authenticating clients. The AAA profile also specifies the default user roles for 802.1x authentication.

To configure the AAA profile:

```
aaa profile aaa_dot1x
    dot1x-default-role guest
    authentication-dot1x dot1x
    dot1x-server-group radiusGuest
```

This chapter describes how to prepare ClearPass for LDAP and SQL authentication.

This chapter includes the following information:

- [LDAP Authentication Source Configuration](#)
- [SQL Authentication Source Configuration](#)

## LDAP Authentication Source Configuration

Policy Manager can perform NTLM/MSCHAPv2, PAP/GTC, and certificate-based authentications against any LDAP-compliant directory (for example, Novell eDirectory, OpenLDAP, and Sun Directory Server).

LDAP and Active Directory-based server configurations are similar. You can retrieve role-mapping attributes by using filters.

### Configuring Generic LDAP Authentication Sources

To configure Generic LDAP authentication sources:

1. Navigate to the **Configuration > Authentication > Sources** page.

The **Authentication Sources > General** page opens.

#### General Page

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

2. Click **Add**.

The **Add Authentication Source** page opens.

**Figure 202** Adding a Generic LDAP Authentication Database

The screenshot shows the 'Authentication Sources' configuration page with the 'General' tab selected. The form fields include:

- Name:** LDAP1
- Description:** (empty text area)
- Type:** Generic LDAP
- Use for Authorization:**  Enable to use this Authentication Source to also fetch role mapping attributes
- Authorization Sources:** A dropdown menu with options: Remove, View Details, and -- Select --. Below this is a list of backup servers with Move Up, Move Down, Add Backup, and Remove buttons.
- Server Timeout:** 10 seconds
- Cache Timeout:** 36000 seconds
- Backup Servers Priority:** (empty list)

- Enter the values for these parameters as described in [Table 68](#).

**Table 68:** General Page Parameters for Generic LDAP Database

Parameter	Action/Description
Name	Enter the name of the LDAP authentication source.
Description	Provide the additional information that helps to identify the LDAP authentication source.
Type	Select <b>Generic LDAP</b> .
Use for Authorization	When <b>Use for Authorization</b> is enabled, ClearPass can use this authentication source to fetch role-mapping attributes. This option is enabled by default.
Backup Servers Priority	To add a backup server in the event the main server goes down, click <b>Add Backup</b> . <b>NOTE:</b> Aruba recommends setting up one or more backup servers.
Authorization Sources	Specifies additional sources from which role-mapping attributes may be fetched. 1. Select a previously configured authentication source from the drop-down list. 2. To add authentication source to the list of authorization sources, click <b>Add</b> . To remove the authentication source from the list, click <b>Remove</b> .

Parameter	Action/Description
	If Policy Manager authenticates the user or device from this authentication source, it also fetches role mapping attributes from these additional authorization sources.
Cache Timeout	Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the duration in number of seconds for which the attributes are cached. The default is <b>36000</b> seconds (one hour).
Backup Servers Priority	<p>To add a backup server, click <b>Add Backup</b>.</p> <p>If the <b>Backup 1</b> tab appears, you can specify connection details for a backup server.</p> <ul style="list-style-type: none"> <li>• To remove a backup server, select the server name and click <b>Remove</b>.</li> <li>• To change the server priority of the backup servers, select <b>Move Up</b> or <b>Move Down</b>.</li> </ul> <p>This is the order in which Policy Manager attempts to connect to the backup servers when the primary server is unreachable.</p>

When satisfied with these settings, click **Next**.

The **Authentication Sources Primary** page opens.

## Primary Page

**Figure 203 Primary Page: Generic LDAP Authentication Database**

Configuration > Authentication > Sources > Add

### Authentication Sources

**For successful authentications, make sure you have the CA cert of the AD/LDAP added to Certificate Trust List**

General	Primary	Attributes	Summary
<b>Connection Details</b> Hostname: <input type="text" value="LDAP1"/> Connection Security: <input type="button" value="LDAP over SSL"/> Port: <input type="text" value="636"/> Verify Server Certificate: <input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection			
Bind DN: <input type="text"/> Bind Password: <input type="password"/>  Base DN: <input type="text"/> <a href="#">Search Base Dn</a> Search Scope: <input type="button" value="SubTree Search"/> LDAP Referrals: <input type="checkbox"/> Follow referrals			
Bind User: <input type="checkbox"/> Allow bind using user password			
Password Attribute: <input type="text" value="userPassword"/> Password Type: <input type="button" value="Cleartext"/> Password Header: <input type="text"/> User Certificate : <input type="text" value="userCertificate"/>			

**Table 69: Primary Parameters for an LDAP Authentication Source**

Parameter	Action/Description
Hostname	<p>Enter the name or IP address of the LDAP server you're going to use for authentication.</p> <p>Note that most domain controllers are also LDAP servers. ClearPass uses LDAP to talk to the domain controller.</p>
Connection Security	<p>Set <b>Connection Security</b> to: <b>LDAP over SSL</b>.</p> <p>This enables the secure sockets layer (SSL) cryptographic protocol to connect to your Active Directory. Selecting <b>LDAP over SSL</b> automatically populates the <i>Port</i> field to <b>636</b>.</p> <p><b>NOTE:</b> 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 <b>636</b>.</p> <p><b>NOTE:</b> To ensure successful authentication, be sure to add the CA certificate of the LDAP server to the Certificate Trust List.</p>
Port	<p>Specify the TCP port at which the LDAP server is listening for connections.</p> <p>For a single domain LDAP Domain Service:</p> <ul style="list-style-type: none"> <li>Default port for LDAP: <b>389</b></li> <li>Default port for LDAP over SSL: <b>636</b></li> </ul> <p>When you set the <i>Connection Security</i> field to <b>AD over SSL</b>, this port is automatically set to <b>636</b>.</p> <p>For a multi-domain LDAP Domain Service forest, the default ports for the global catalog are:</p> <ul style="list-style-type: none"> <li>Default port without SSL: <b>3268</b></li> <li>Default port with SSL: <b>3269</b></li> </ul>
Verify Server Certificate	Enable this option to verify the Server Certificate for a secure connection.
Bind DN	<p>Enter the Distinguished Name of the node in your directory tree from which to start searching for records.</p> <p>The Bind DN text box specifies the full distinguished name (DN), including common name (CN), of an LDAP user account that has privileges to search for users (usually the Administrator account). For example:</p> <p>CN=Administrator,CN=Users,DC=mycompany,DC=com</p> <p><b>NOTE:</b> You may need to get the Bind DN from the LDAP administrator.</p> <p>This user account must have at least domain user privileges.</p> <p>The Bind DN user, such as Administrator, is the username associated with the Bind DN user account.</p> <ul style="list-style-type: none"> <li>For a single domain LDAP Domain Service, the Bind DN entry must be located in the same branch and below the Base DN.</li> </ul>

Parameter	Action/Description
	<ul style="list-style-type: none"> <li>For a multi-domain LDAP Domain Service forest, because you leave the Base DN text box empty, the restrictions that apply for a single domain do not apply for a multi-domain forest.</li> </ul> <p>ClearPass fills in the domain portion of the Bind DN.</p> <ol style="list-style-type: none"> <li>Specify the username. ClearPass also populates the <i>Base DN</i>, and the <i>NetBIOS Domain Name</i> fields.</li> </ol> <p>For related information, see <a href="#">LDAP Authentication Source Configuration</a>.</p>
Bind Password	<p>This is the text box for the Active Directory password for the account that can search for users.</p> <p>Enter the Bind password.</p> <p><b>NOTE:</b> The Bind password is the same password used in association with the Bind DN user account.</p>
NetBIOS Domain Name	<p>Specify the DN (Distinguished Name) of the administrator account. ClearPass uses this account to access all other records in the directory.</p> <p><b>NOTE:</b> For Active Directory, the bind DN can also be in the administrator@domain format (for example, administrator@acme.com).</p>
Base DN	<p>For a single domain Active Directory Domain Service, this is the text box for the Distinguished Name (DN) of the starting point for directory server searches. For example:</p> <p style="padding-left: 40px;">DC=mycompany,DC=com</p> <p>The LDAP server starts from this DN to create master lists from which you can later filter out individual users and groups.</p> <p><b>NOTE:</b> The Base DN value that is automatically populated in this instance is <i>not</i> the best practice Base DN value.</p> <p>Aruba recommends that you narrow down the Base DN as far as possible to reduce the load on the Active Directory LDAP server. For example, if all your users are in the AD Users and Computer Users folder, then set the Base DN to search in the Users folder.</p> <ol style="list-style-type: none"> <li>To browse the LDAP directory hierarchy, click <b>Search Base DN</b>. The LDAP Browser opens.</li> <li>Navigate to the DN you want to use as the Base DN.</li> <li>To select a node as a Base DN, click the appropriate node in the tree structure.</li> <li>For a multi-domain Active Directory Domain Service (AD DS) forest, the appropriate action is to leave the Base DN text box blank.</li> </ol> <p><b>NOTE:</b> This is also one way to test the connectivity to your LDAP directory. If the values entered for the primary server attributes are correct, you should be able to browse the directory hierarchy by clicking <b>Search Base DN</b>.</p>
Search Scope	<p>Search scope is related to the Base DN. The search scope defines how LDAP will search for your objects.</p> <p>Select the <b>Search Scope</b>.</p> <ul style="list-style-type: none"> <li>Subtree Search: Searches every object and sub-object in the LDAP directory.</li> </ul>

Parameter	Action/Description
	<ul style="list-style-type: none"> <li>One-Level Search: Looks directly under the Base DN.</li> <li>Base Object: Searches any object under the Base DN.</li> </ul>
LDAP Referrals	<p>Aruba does <i>not</i> recommend enabling the "Follow Referrals" check box.</p> <p>This function directs the LDAP server to find a specific user in its tree, but it's possible for the user to be included on another LDAP server, which can cause a search loop.</p>
Bind User	<p>Enable this option to allow a bind operation using the user password.</p> <p>For clients to be authenticated by using the LDAP bind method, Policy Manager must receive the password in clear text.</p>
Password Attribute	Enter the name of the attribute in the user record from which the user password can be retrieved.
Password Type	Specify the password type: <b>Cleartext, NT Hash, LM Hash, SHA1, SHA256, MD5</b> .
Password Header	<p>Oracle's LDAP implementation prepends a header to a hashed password string.</p> <p>If you are using Oracle LDAP, enter the header in this field so the hashed password can be correctly identified and read.</p>
User Certificate	Leave the value that is automatically populated in this field as the default unless your LDAP administrator has a different attribute for storing the user certificate.
Always use NetBIOS name	<p>Check this option to always use the NetBIOS name instead of the domain part in the username for authentication.</p> <p><b>NOTE:</b> This field is available only if you select <b>Active Directory</b> as an authentication source.</p>

When satisfied with these settings, click **Next**.

The **Summary** page is displayed, which shows all the settings you have entered for the LDAP authentication source.

## SQL Authentication Source Configuration

This section includes the following information:

- [Configuring a Generic SQL Authentication Source](#)
- [Defining a Filter Query](#)

### Configuring a Generic SQL Authentication Source

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.

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

- You can configure the primary and backup servers, session details, filter query, and role mapping attributes to fetch the generic SQL authentication sources.

To configure a generic SQL authentication source:

1. Navigate to **Configuration > Authentication > Sources**.

The **Authentication Sources** page opens.

2. Click **Add**.

The **Authentication Sources > General** page opens.

## General Page

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

**Figure 204** General Page: Generic SQL Authentication Database

Configuration » Authentication » Sources » Add

Authentication Sources

General		Primary	Attributes	Summary
Name:	<input type="text"/>			
Description:	<input type="text"/>			
Type:	<input type="text" value="Generic SQL DB"/>			
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes			
Authorization Sources:	<input type="button" value="Remove"/> <input type="button" value="View Details"/> <input type="button" value="-- Select --"/>			
Cache Timeout:	36000 seconds			
Backup Servers Priority:	<input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add Backup"/> <input type="button" value="Remove"/>			
<a href="#">Back to Authentication Sources</a>		<input type="button" value="Next &gt;"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/>		

3. Enter the information for each of the required parameters as described in [Table 70](#).

**Table 70:** General Page Parameters for Generic SQL Database

Parameter	Action/Description
Name	1. Enter the name of the SQL authentication source.
Description	2. Provide the additional information that helps to identify the authentication source.
Type	3. Select <b>Generic SQL DB</b> .
Use for Authorization	4. Leave the <b>Use for Authorization</b> setting enabled. When <b>Use for Authorization</b> is enabled, ClearPass can use this authentication

Parameter	Action/Description
	source to fetch role-mapping attributes. This option is enabled by default.
Backup Servers Priority	5. To add a backup server in the event the main server goes down, click <b>Add Backup</b> . <b>NOTE:</b> Aruba recommends setting up one or more backup servers.
Authorization Sources	6. Specify additional sources from which role-mapping attributes can be fetched. <ul style="list-style-type: none"><li>● Select a previously configured authentication source from the drop-down list.</li><li>● To add authentication source to the list of authorization sources, click <b>Add</b>.</li><li>● To remove the authentication source from the list, click <b>Remove</b>.</li></ul> If Policy Manager authenticates the user or device from this authentication source, it also fetches role mapping attributes from these additional authorization sources.
Cache Timeout	7. Specify the number of seconds for the <b>Cache Timeout</b> . Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the duration in number of seconds for which the attributes are cached.
Backup Servers Priority	8. To add a backup server, click <b>Add Backup</b> . If the <b>Backup 1</b> tab appears, you can specify connection details for a backup server. <ul style="list-style-type: none"><li>● To remove a backup server, select the server name and click <b>Remove</b>.</li><li>● To change the server priority of the backup servers, select <b>Move Up</b> or <b>Move Down</b>.</li></ul> This is the order in which Policy Manager attempts to connect to the backup servers when the primary server is unreachable.
	9. When satisfied with these settings, click <b>Next</b> . The Authentication Sources <b>Primary</b> page opens.

## Primary Page

**Figure 205 Primary Page: Generic SQL Authentication Source**

Configuration » Authentication » Sources » Add

### Authentication Sources

General	Primary	Attributes	Summary																
<b>Connection Details</b> <table border="1"> <tr> <td>Server Name:</td> <td><input type="text"/></td> </tr> <tr> <td>Port (Optional):</td> <td><input type="text"/> (Specify only if you want to override the default value)</td> </tr> <tr> <td>Database Name:</td> <td><input type="text"/></td> </tr> <tr> <td>Login Username:</td> <td><input type="text"/></td> </tr> <tr> <td>Login Password:</td> <td><input type="password"/></td> </tr> <tr> <td>Timeout:</td> <td>10 seconds</td> </tr> <tr> <td>ODBC Driver:</td> <td><input type="text"/> PostgreSQL</td> </tr> <tr> <td>Password Type:</td> <td><input type="text"/> Cleartext</td> </tr> </table>				Server Name:	<input type="text"/>	Port (Optional):	<input type="text"/> (Specify only if you want to override the default value)	Database Name:	<input type="text"/>	Login Username:	<input type="text"/>	Login Password:	<input type="password"/>	Timeout:	10 seconds	ODBC Driver:	<input type="text"/> PostgreSQL	Password Type:	<input type="text"/> Cleartext
Server Name:	<input type="text"/>																		
Port (Optional):	<input type="text"/> (Specify only if you want to override the default value)																		
Database Name:	<input type="text"/>																		
Login Username:	<input type="text"/>																		
Login Password:	<input type="password"/>																		
Timeout:	10 seconds																		
ODBC Driver:	<input type="text"/> PostgreSQL																		
Password Type:	<input type="text"/> Cleartext																		
<a href="#">Back to Authentication Sources</a> <span style="float: right;">Next &gt; Save Cancel</span>																			

10. Enter the information for each of the required parameters as described in [Table 71](#).

**Table 71: Primary Page Parameters for Generic SQL Database**

Parameter	Action/Description
Server Name	Enter the name or IP address of the Generic SQL server you're going to use for authentication.
Port	Optionally, you can specify a port value to override the default port.
Database Name	Enter the name of the database from which records can be retrieved.
Login Username	Enter the name of the user used to log into the database. This account must have read access to all the attributes that need to be retrieved by the specified filters.
Password	Enter the password for the user account entered in the <i>Login Username</i> field.
Timeout	Enter the duration in 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).
ODBC Driver	<p>Select the ODBC driver to connect to the database.</p> <ul style="list-style-type: none"><li>● PostgreSQL</li><li>● Oracle 11g</li><li>● MariaDB</li><li>● MSSQL</li></ul> <p><b>NOTE:</b> MySQL is no longer supported for ClearPass 6.7.x and later. MySQL has been replaced by Maria-DB Connector (MariaDB).</p> <p>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:</p> <ul style="list-style-type: none"><li>● Backslash (\ )</li><li>● At-sign (@)</li><li>● Hyphen</li><li>● Underscore</li></ul>
Password Type	Specify how the user password is stored in the database: <ul style="list-style-type: none"><li>● Cleartext : Password is stored as clear, unencrypted text.</li><li>● NT Hash: Password is stored with an NT hash using MD4.</li><li>● LM Hash : Password is stored with a LAN Manager Hash using DES.</li><li>● SHA: Password is stored with a Secure Hash Algorighm (SHA) hash.</li><li>● SHA256: Password is stored with an SHA-256 hash function.</li><li>● MD5</li></ul>

11. When satisfied with the **Primary** page settings, click **Next**.

The Attributes page appears.

## Attributes Page

The **Attributes** page defines the SQL database query filters and the attributes to be fetched when using those filters.

**Figure 206** Attributes Page: Generic SQL Authentication Source

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

**Add More Filters**

**Back to Authentication Sources**    **Next >**    **Save**    **Cancel**

12. Enter the information for each of the required parameters as described in [Table 72](#).

**Table 72:** Attributes Page Parameters for Generic SQL Database

Parameter	Action/Description
Filter Name	Displays the name of the filter.
Attribute Name	Specifies the name of the SQL database attributes defined for this filter.
Alias Name	Specifies an alias name for each attribute name selected for the filter.
Enabled As	Optionally, indicates whether the filter is enabled as a role or an attribute type. This option can also be blank.
Add More Filters	Click this button to open the <b>Configure Filter</b> page (for details, see the next section, <a href="#">Defining a Filter Query</a> ). Use this page to define a filter query and the related attributes to be fetched from the SQL DB store.

13. When satisfied with the **Attribute** page settings, click **Next**.

The Summary page appears.

## Defining a Filter Query

The Configure Filter page allows you to define a filter query and the related attributes to be fetched from the SQL DB store.

To define a filter query:

1. Navigate to **Configuration > Authentication > Sources**.

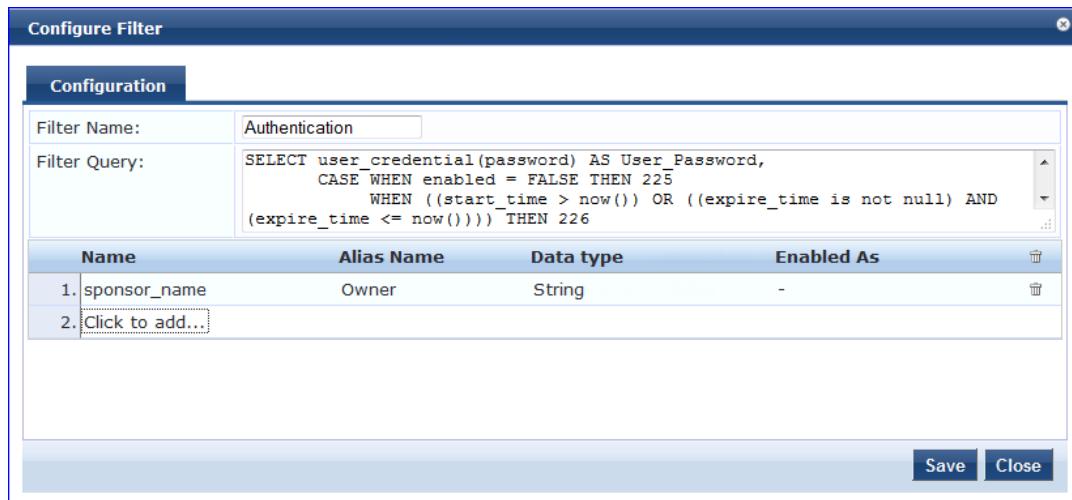
The **Authentication Sources** page opens.

- a. If you're defining a new filter for an existing authentication source, click the name of the authentication source, then select the **Attributes** tab.
- b. If you're defining a new filter query for a newly configured authentication source, follow the steps described in the previous section.

2. From the **Attributes** page, click **Add More Filters**.

The **Configure Filter** page opens.

**Figure 207** Configure Filter Page: Generic SQL Authentication Source



3. Enter the information for each of the required parameters as described in [Table 73](#).

**Table 73:** Configure Filter Page Parameters for Generic SQL Database

Parameter	Action/Description
Filter Name	Enter the name of the new filter.
Filter Query	Specify an SQL query to fetch the attributes from the user or device record in the database.
Name	Select Click to add to specify the name of the attribute.
Alias Name	Specify the alias name for the attribute. By default, this is the same value as the attribute name.
Data Type	Specify the data type for this attribute, such as String, Integer, or Boolean.
Enabled As	Specify whether this value is to be used directly as a role or an attribute in an Enforcement Policy. This option bypasses having to assign a role in Policy Manager through a Role Mapping Policy.

4. When satisfied with the **Configure Filter** page settings, click **Save**.



This chapter includes the following information:

- [A Tour of the EAP-PEAP-MSCHAPv2 Ladder](#)

## A Tour of the EAP-PEAP-MSCHAPv2 Ladder

This section contains the following information:

- [About EAP-PEAP MSCHAPv2](#)
- [EAP-PEAP MSCHAPv2 Handshake Exchange Summary](#)

### About EAP-PEAP MSCHAPv2

The authenticated wireless access design based on Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2 (PEAP-MS-CHAPv2) utilizes the user account credentials (user name and password) stored in Active Directory Domain Services to authenticate wireless access clients, instead of using smart cards or user and computer certificates for client authentication.

### EAP-PEAP MSCHAPv2 Handshake Exchange Summary

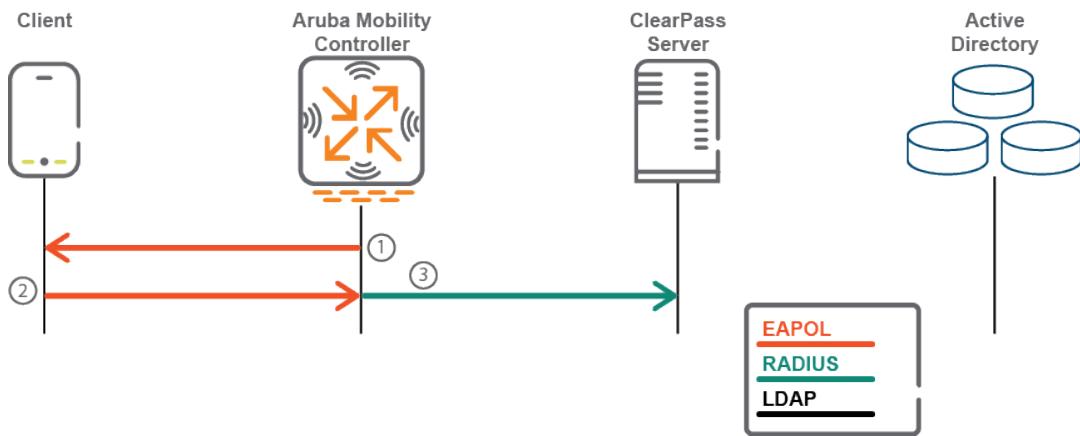
[Table 74](#) describes how a typical 802.1X authentication session flows when using ClearPass as the authentication server with Microsoft Active Directory as the back-end user identity repository.

- The term **supplicant** refers to a client device, such as a laptop, tablet, or mobile phone requesting access to a network.
- The term **authenticator** refers to a network device, such as an Aruba Mobility Controller or an Instant Access Point (AP), which controls access to a network resource.
- The term **authentication server** refers to the ClearPass Policy Manager server, which processes the authentication requests and provides either an accept or reject response.

Each section of [Table 74](#) is followed by a diagram that illustrates the communication steps between the devices described in the table. The numbers of each step in the table correspond to the numbers assigned to the handshake sequences in the accompanying illustrations.

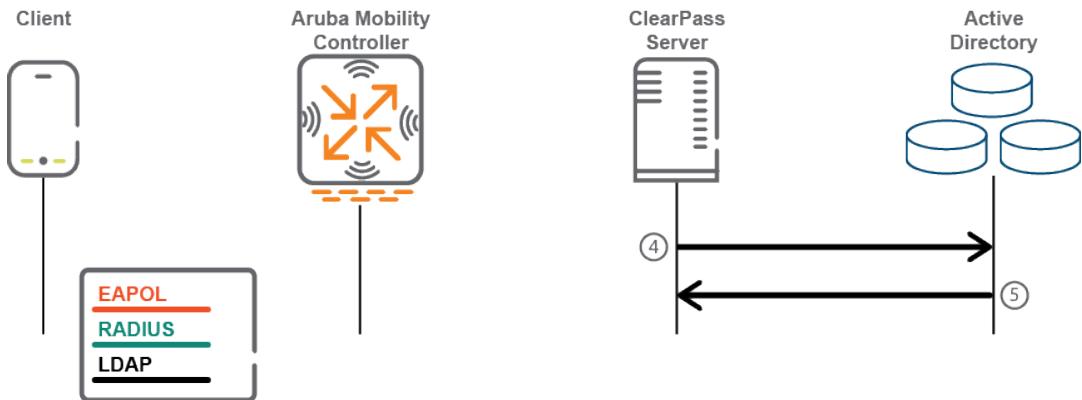
**Table 74: Detailed Sequence of the EAP-PEAP-Active Directory Handshake Exchange**

Extensible Authentication Protocol over LAN (EAPOL) Start	
1	The authenticator sends an EAP-Request for the identity of the connecting supplicant (client device).
2	The supplicant responds to the authenticator with an EAP Identity Response that contains the identity (username) used for authentication. This is referred to as the "Outer Identity."
3	The authenticator forwards the EAP Identity Response with the identity of the user to the authentication server (ClearPass Policy Manager).



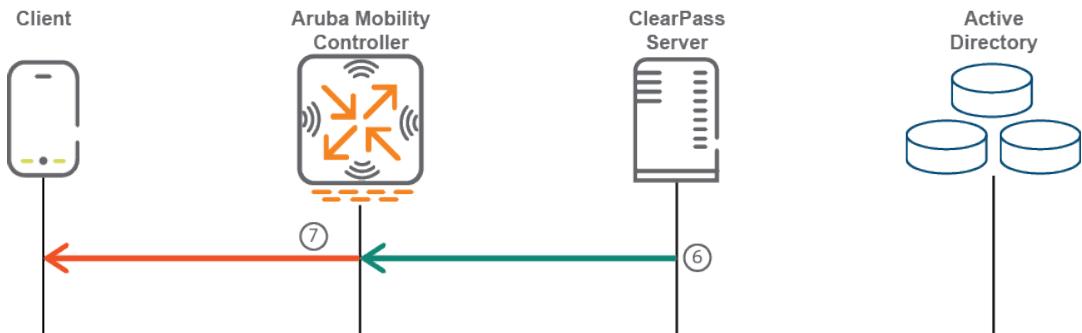
#### Active Directory

Active Directory	
4	The authentication server performs an LDAP lookup against its configured Active Directory authentication sources to try to find the user's name in the directory, along with some basic LDAP attributes, such as <i>sAMAccountName</i> .
5	The LDAP server responds to the authentication server's LDAP search request with the appropriate answers to the LDAP lookup.



## EAPOL

6	The authentication server responds to the supplicant through the authenticator with an EAP-Request message indicating that it would like to initiate EAP-PEAP.
7	The authenticator passes the EAP-Request message to the supplicant.

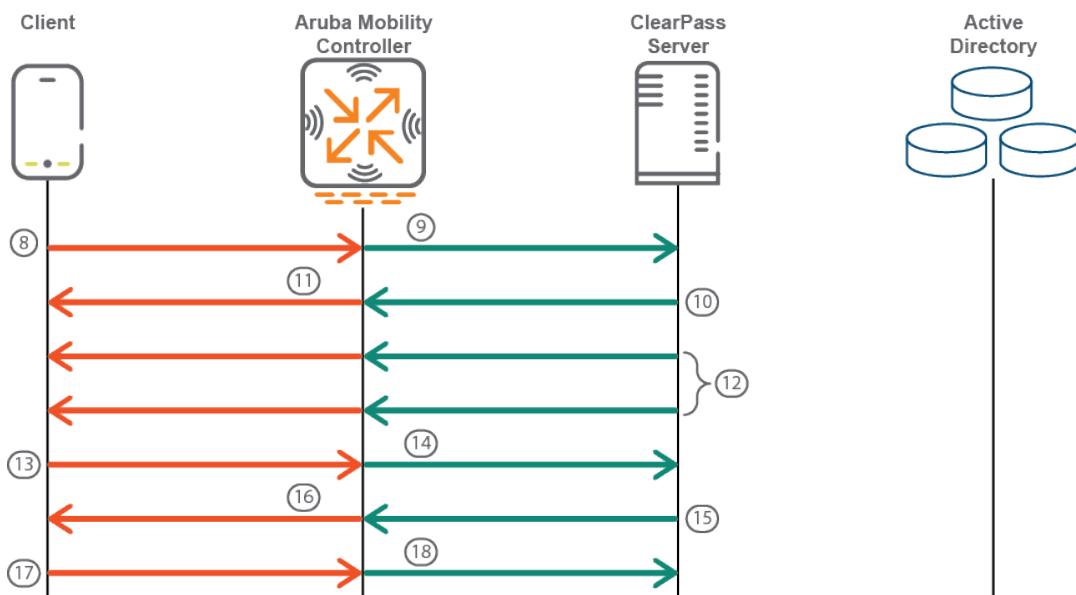


## Transport Layer Security (TLS) Tunnel Setup

8	The supplicant sends a Transport Layer Security (TLS) "Client Hello" message within an EAP-response message through the authenticator to the authentication server.
9	The authenticator passes the EAP-Response message containing the TLS Client Hello message to the authentication server.
10	The authentication server responds with a TLS Handshake message of types "Server Hello," "Certificate," "Server Key Exchange," and "Server Hello Done" to the authenticator.
11	The authenticator forwards the TLS handshake messages between the authentication server and the supplicant inside of EAP Request (server) and EAP Response (supplicant) messages.

## Transport Layer Security (TLS) Tunnel Setup

12	Steps 10 and 11 repeat until the authentication server has transmitted all of its handshake messages. This may take several steps due to having to dismantle the certificates into fragments that fit within the size limits of an EAP message.
13	The supplicant sends another TLS Handshake message inside an EAP-Response message of types "Client Key Exchange," "Change Cipher Spec," "Handshake," and "Client Finished" to the authenticator.
14	The authenticator sends this EAP-Response to the authentication server.
14	The authentication server responds to the authenticator with an EAP-Request for the supplicant that contains the message types "Change Cipher Spec" and "Server Finished."
16	The authenticator passes the EAP message to the supplicant.
17	The supplicant sends an EAP-Response for the authentication server to the authenticator.
18	The authenticator sends the EAP-Response to the authentication server.

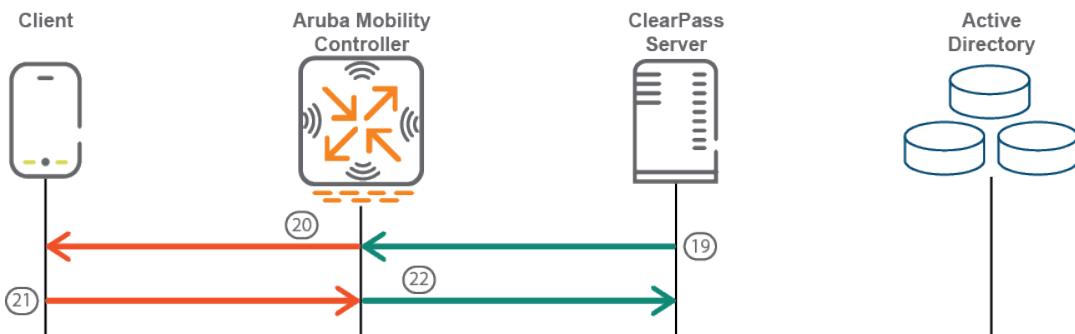


## Inner EAP MSCHAPv2

19	Inside the TLS tunnel, the EAP process starts again with the authentication server sending an EAP Identity Request to the supplicant requesting the client's identity.
----	--

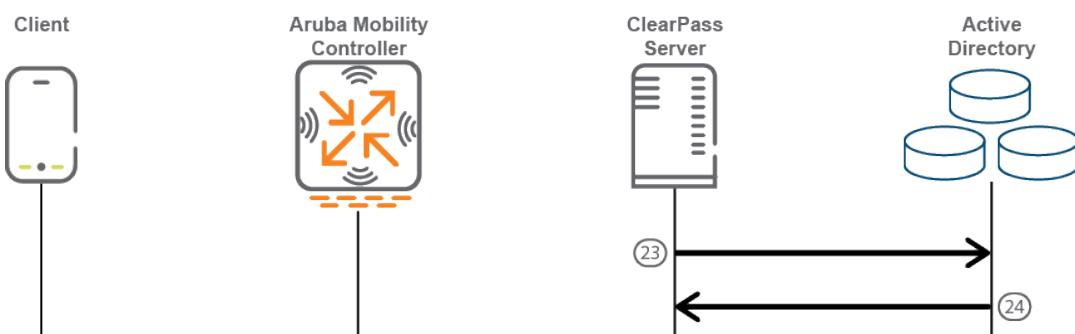
## Inner EAP MSCHAPv2

20	The authenticator sends the EAP Identity Request message to the supplicant requesting the client's identity.
21	The supplicant responds with an EAP Identity Response containing its identity to the authenticator.
22	The authenticator forwards this EAP Identity Response to the authentication server.



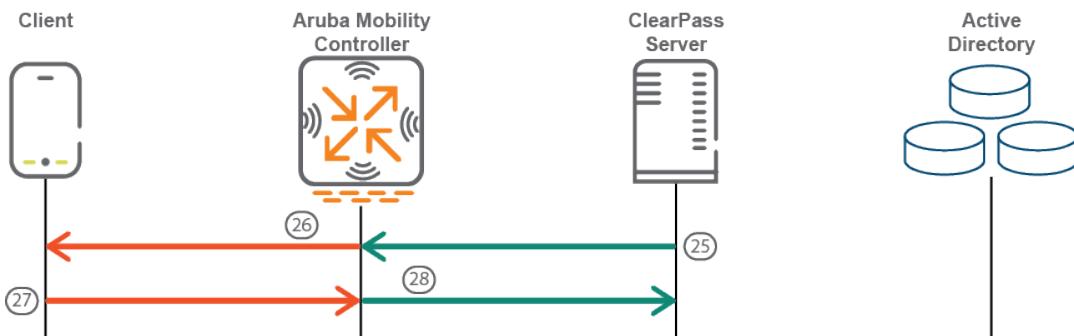
## Active Directory

23	The authentication server performs an LDAP lookup against its configured Active Directory authentication sources to try to find the user's name in the directory, along with some basic LDAP attributes, such as <i>sAMAccountName</i> .
24	The LDAP server responds to the LDAP search request with the appropriate answers to the query.



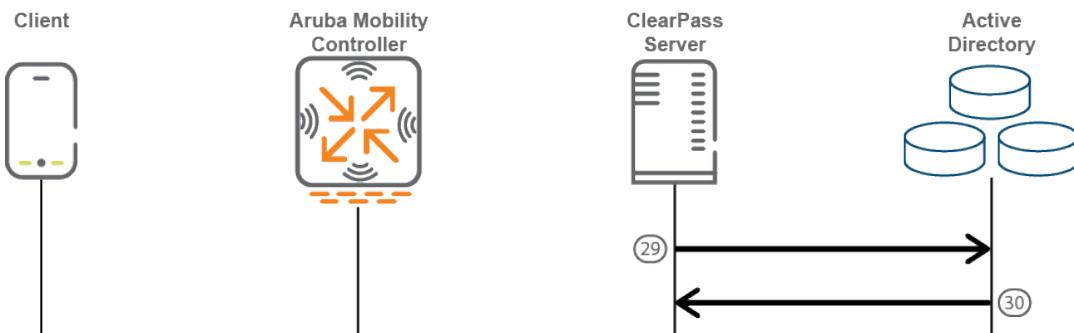
## Inner EAP MSCHAPv2

25	The authentication server sends an EAP request to the supplicant containing an MS-CHAPv2 challenge.
26	The authenticator forwards the EAP request to the supplicant.
27	The supplicant responds with an EAP Identity Response containing its identity to the authenticator.
28	The authenticator forwards this EAP Identity Response to the authentication server.



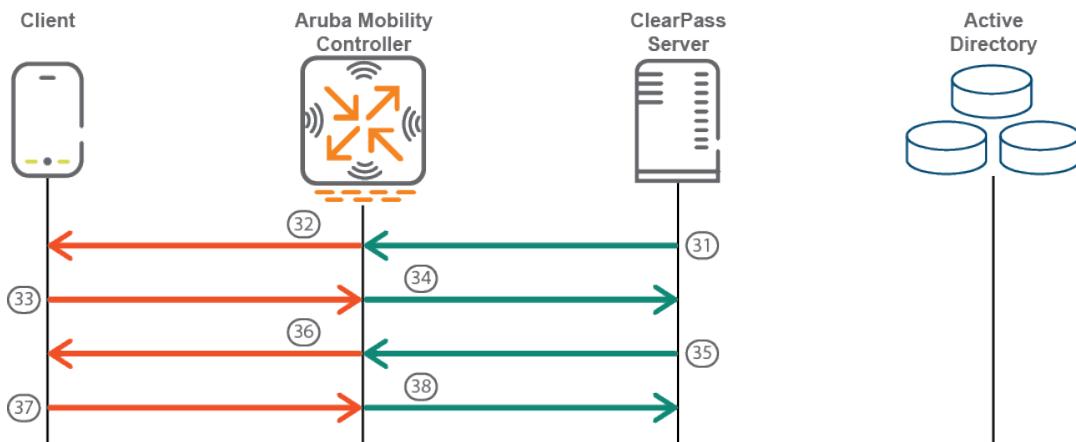
## Active Directory

29	The authentication server takes the username and the MSCHAPv2 response from the supplicant and combines it with the MSCHAPv2 challenge and the NetBIOS name of the Active Directory domain and submits this set of information to the Active Directory domain controller for authentication. This is done via NT LAN Manager (NTLM).
30	The Active Directory domain controller lets the authentication server know that the authentication was successful.



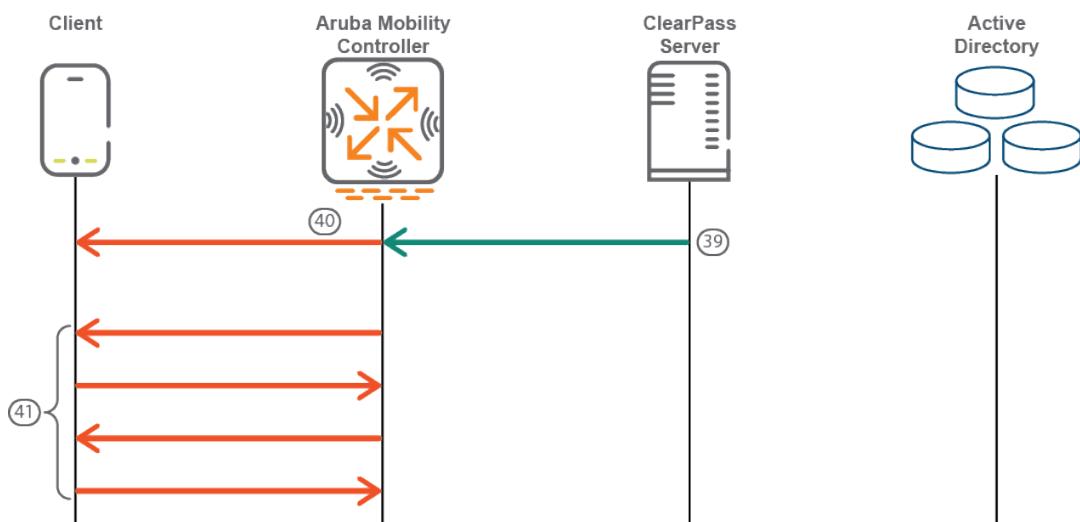
## Inner EAP MSCHAPv2

31	The authentication server sends an EAP-Request message for the supplicant with an MSCHAPv2 success message and an authenticator response string from the Active Directory Domain Controller to the authenticator.
32	The authenticator passes the EAP-Request with an MSCHAPv2 success message and the authenticator response to the supplicant.
33	The supplicant sends an EAP-Response message for the authentication server with an MSCHAPv2 success message to the authenticator.
34	The authenticator sends the EAP-Response message from the supplicant with the MSCHAPv2 success message to the authentication server.
35	The authentication server sends an EAP-Request message to the authenticator indicating that the Inner EAP method was successful.
36	The authenticator forwards this EAP-Request to the supplicant.
37	The supplicant sends an EAP-Response to the authentication server, acknowledging that the Inner EAP method was successful.
38	The authenticator forwards the EAP-Response from the the supplicant to the authentication server.



## EAPOL

	<b>39</b>	The authentication server sends a RADIUS access-accept message to the authenticator with an EAPOL success message along with the key material.
	<b>40</b>	The authenticator sends an EAPOL success message to the supplicant.
	<b>41</b>	The authenticator and supplicant complete a four-way handshake to start the flow of encrypted wireless traffic.



This chapter includes the following information:

- [ClearPass Configuration API Overview](#)
- [ClearPass Configuration API Methods](#)
- [ClearPass Configuration API Examples](#)
- [API Error Handling](#)
- [About the API Explorer](#)

## ClearPass Configuration API Overview

This section contains the following information:

- [Introduction](#)
- [Admin Accounts for API Access](#)
- [XML Data Structure](#)
- [Filter Elements](#)
- [Advanced Match Operations](#)
- [Setting Up Bulk Access for Endpoints and Guest Accounts](#)

### Introduction

The ClearPass Configuration Application Programming Interface (API) is used to read and write a number of configuration elements (known as *Entities*), either programmatically or by using a script.

The ClearPass Configuration API allows you to configure or modify the entities in ClearPass without logging into the Admin user interface. For example, when you create a new user in the database, you may want to create a guest user automatically. You can use the ClearPass Configuration API to automate this task.

The API is made available through an HTTP POST-based mechanism. The API request is in the form of an XML snippet that is posted to a URL hosted by an administration server on the ClearPass Policy Manager server.

The API response received is also in the form of an XML snippet. Both the XML request and the XML response are structurally defined in an XSD-format file.

**Read, Write, and Delete** operations are supported in the ClearPass Configuration API. These operations are referred to as "methods." You can use these methods to perform the following name-list based operations:

- **NameList.** Returns the list of names for all objects created for an Entity type.
- **Reorder.** Receives a list of names of Entity type objects and applies the new order to the list of objects.
- **Status Change.** Retrieves the name-list of disabled and enabled entities of a specific type and changes the status of the entities appropriately.

Every XML request must conform to the ClearPass Configuration API XML schema.

### Admin Accounts for API Access

Only the configured Admin users can use API access. Rather than using the default **admin** user account, it is recommended that you create a separate user for API access.

To create a new user for API access, update the password of the default **apiadmin** user account or create a new Admin user with only API access privileges.

This ensures that all API actions are tracked through the **Audit Viewer** page for this user account.

Additionally, restrictions to specific entities can be enforced by defining a custom admin privilege level and creating API admin users with that privilege level. This ensures that the API account included in client scripts secure the confidential information in the system.

## XML Data Structure

The following elements define the structure of XML data:

- **Root:** The root element is `<TipsApiRequest>` for a request and `<TipsApiResponse>` for a response.
- **Sub-element:** `<TipsHeader>` describes the version (for example 3.0). The **sub-element** is the container object that can be controlled by adding and modifying attributes. The sub-element in the XML request contains only the version number; the sub-element in the XML response contains the version number, time of execution (exportTime), and entity types.
- **Body:** Describes the child elements of XML data that are known the **body**. The body contains the **Filter** elements in the XML request and a list of **Entity** objects in the XML response.

[Figure 208](#) describes the structure of XML data in an XML request:

**Figure 208** Structure of an XML Request

The diagram shows the structure of an XML request. It consists of three main parts: a yellow highlighted area at the top containing the root element `<TipsApiRequest>`, a blue highlighted area in the middle containing the sub-element `<TipsHeader>`, and a green highlighted area at the bottom containing the body elements `<Filter>` and `</Filter>`. Red arrows point from the labels "Root", "Sub-element", and "Body" to their respective highlighted areas.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
  <TipsHeader version="3.0"/>
  <Filter entity="NadClient">
    <Criteria fieldName="ipAddress" filterString="192.168.16.x" match="contains">
      <MoreFilterConditions fieldName="name" fieldValue="IETF" match="equals"/>
    </Criteria>
  </Filter>
</TipsApiRequest>
```

[Figure 209](#) describes the structure of XML data in an XML response:

**Figure 209** Structure of an XML Response

The diagram shows the structure of an XML response. It consists of three main parts: a yellow highlighted area at the top containing the root element `<TipsApiResponse>`, a blue highlighted area in the middle containing the sub-element `<TipsHeader>`, and a green highlighted area at the bottom containing the body elements `<GuestUsers>` and `</GuestUsers>`. Red arrows point from the labels "Root", "Sub-element", and "Body" to their respective highlighted areas.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDcfs/1.0">
  <TipsHeader exportTime="Thu Sep 30 10:47:26 IST 2010" version="3.0"/>
  <StatusCode>Success</StatusCode>
  <EntityMaxRecordCount>1</EntityMaxRecordCount>
  <GuestUsers>
    <GuestUser enabled="true" expiryTime="2010-12-29 12:24:37.0" startTime="2010-09-29
12:26:08.28" sponsorName="admin" guestType="USER" password="avenda123#" name="kang">
      <GuestUserDetails sendSms="false" sendEmail="true" description="Test"/>
      <GuestUserTags tagName="Company Name" tagValue="Avenda Systems"/>
      <GuestUserTags tagName="Email Address" tagValue="kang@sample.net"/>
      <GuestUserTags tagName="Location" tagValue="Room A"/>
    </GuestUser>
  </GuestUsers>
</TipsApiResponse>
```

## Filter Elements

Use the **Filter** element to fetch a list of objects of a specific entity. You can use a filter to perform **Read** and **Delete** operations.

A filter contains a **Criteria** element that includes the following:

- **fieldname**: Specifies the name of the field present in XML that needs to be filtered.
- **filterString**: Specifies the string that is used to match the filter during a match of the filter.
- **match**: Specifies the operator to be used.

For example, the match operator equals/matches the value of the **fieldname** field in the Entity object using **filterString**.

## Filter Example

The following is an example of an XML request that contains a filter on a Guest user with a criteria to fetch Guest users that match the name **McIntosh**.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0" source="Guest"/>
<Filter entity="GuestUser">
<Criteria fieldName="name" filterString="McIntosh" match="equals"/>
</Filter>
</TipsApiRequest>
```

## Advanced Match Operations

When you specify multiple filters, the result can be a combination of the list of elements of all of the filter criteria. For **Match All** criteria, specify the nested criteria as **MoreFilterConditions**. For match any criteria, multiple filters with criteria can be specified for the Entity type. If a criteria is not specified, then the **Advanced Match** operation fetches all objects of the Entity type.



---

Because the number of entities and the associated tag attributes with each entity can impact performance, the complex query supported in the Advanced Match Operations should be used with care.

---

You can use the API to query based on tag attributes when the queries are not repeated.

With the XML request and response examples given in this section, you can use the **Advanced Match** operation to fetch all objects of an Entity type.

## XML Request

The following example describes the XML request that fetches all network devices with the IP address 192.0.2.10 and vendor IETF:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0"/>
<Filter entity="NadClient">
<Criteria fieldName="ipAddress" filterString="192.0.2.10" match="contains">
<MoreFilterConditions fieldName="name" fieldValue="IETF" match="equals"/>
</Criteria>
</Filter>
</TipsApiRequest>
```

## Filtering Based on Tag Attributes

The following entity types support tag attributes:

- Endpoint
- Device
- GuestUser
- LocalUser

To filter based on the tag attributes, include an additional attribute called **dataType="ATTRIBUTE"** for that filter condition as described in the following example:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0"/>
<Filter entity="NadClient">
<Criteria fieldName="ipAddress" filterString="192.0.2.10" match="contains">
<MoreFilterConditions fieldName="TagName" fieldValue="TagValue" match="equals"
dataType="ATTRIBUTE"/>
</Criteria>
</Filter>
</TipsApiRequest>
```

## Match Operators Supported in a Criteria

The following match operators are supported in a criteria:

- **equals**: The value of fieldName matches the filterString exactly.
- **notequals**: The value of fieldName does not exactly match the filterString
- **contains**: The value of fieldName partially matches with the filterString, which is case sensitive
- **icontains**: The case insensitive version of **contains**.
- **belongsto**: The value of fieldName is one of the values specified in the filterString, which can be comma separated in this case.

## Setting Up Bulk Access for Endpoints and Guest Accounts

Depending on the deployment, entities such as Endpoints and Guest users can grow to many thousands. These entities support tag attributes, which are custom key-value pairs added by the system or the Administrator that provide more context to the entity.

A bulk query to fetch all the details of the endpoints or Guest users in the system can impact system performance. For better query performance and minimal load on the system, we recommends that you use the bulk query cautiously.

Alternatively, you can primarily use the NameList query followed by a query on individual details for each name present in the NameList. The NameList response depends on the specific endpoint.

## Fetching List of MAC Addresses

Use the following command to fetch the list of MAC addresses for the endpoints present in the system:

```
wget --no-check-certificate --http-user=<USER> --http-password=<PASSWORD> --post-file=in.xml
https://CPPM-Server/tipsapi/config/namelist/Endpoint
```

## NameList Method XML Request

The following is an example of the XML request for the Namelist method:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0"/>
<EntityNameList entity="Endpoint"/>
</TipsApiRequest>

```

## NameList Method XML Response

The following is an example of the Namelist method XML response:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Mon Aug 22 13:37:13 PST 2016" version="6.x"/>
<StatusCode>Success</StatusCode>
<EntityNameList entity="Endpoint">
<Name>000c29eff62f</Name>
<Name>001122aabbc</Name>
</EntityNameList>
</TipsApiResponse>

```

## Fetching List of Endpoints for MAC Address

Use the following command to fetch the list of endpoints for a specific MAC address:

```
wget --no-check-certificate --http-user=<USER> --http-password=<PASSWORD> https://CPPM-Server/tipsapi/config/read/Endpoint>equals?macAddress=000c29eff62f
```

## NameList Method XML Response

The following is an example of the Namelist method XML response:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Mon Aug 22 14:50:09 PST 2016" version="6.x"/>
<StatusCode>Success</StatusCode>
<EntityMaxRecordCount>1</EntityMaxRecordCount>
<Endpoints>
<Endpoint macAddress="000c29eff62f" status="Known"/>
<EndpointTags tagValue="true" tagName="Encryption Enabled"/>
<EndpointTags tagValue="PDA 2" tagName="Phone Number"/>
<EndpointTags tagValue="MobileIron" tagName="Source"/>
<EndpointTags tagValue="3fbe0a80-e7d2-4048-bd2e-62aec232a236" tagName="MDM Identifier"/>
<EndpointTags tagValue="Bala" tagName="Display Name"/>
<EndpointTags tagValue="iPad 2" tagName="Model"/>
<EndpointTags tagValue="true" tagName="MDM Enabled"/>
<EndpointTags tagValue="balu" tagName="Owner"/>
<EndpointTags tagValue="Installed" tagName="Required App"/>
<EndpointTags tagValue="b786da8ca3969e0134f058ca5efe94687ab7f31f" tagName="UDID"/>
<EndpointTags tagValue="iOS 9.3" tagName="OS Version"/>
<EndpointTags tagValue="PDA" tagName="Carrier"/>
<EndpointTags tagValue="false" tagName="Compromised"/>
<EndpointTags tagValue="Corporate" tagName="Ownership"/>
<EndpointTags tagValue="false" tagName="Blacklisted App"/>
<EndpointTags tagValue="Apple" tagName="Manufacturer"/>

```

```
</Endpoint>
</Endpoints>
</TipsApiResponse>
```

## ClearPass Configuration API Methods

This section contains the following information:

- [Introduction](#)
- [Authentication Credentials](#)
- [Entity Names Supported](#)
- [NameList](#)
- [Reorder](#)
- [Status Change](#)

### Introduction

The model for the ClearPass Configuration API is a Representational State Transfer (REST) API, where each method is represented by a URL.

For each operation, an XML request is posted to a different URL identified by the following methods:

- **Read:** The Read method gets one or more filter elements and returns a unified list of Entity objects. The URL for the Read method is:  
*https://<server>/tipsapi/config/read/<Entity>*
- **Write:** The Write method retrieves a list of Entity objects to save. The operation either adds a new object or updates an existing one. The URL for the Write method is:  
*https://<server>/tipsapi/config/write/<Entity>*
- **Delete:** The Delete method executes the following tasks:
  - Initially, the **deleteConfirm** method returns a list of identifiers for each object that needs to be deleted. The URL for the **deleteConfirm** method is:  
*https://<server>/tipsapi/config/deleteConfirm/<Entity>*
  - Creates a second request that contains the list of identifiers to delete. The URL for the Delete method is:  
*https://<server>/tipsapi/config/delete/<Entity>*

### Authentication Credentials

API methods require authorization, which is performed using HTTP basic authentication. The username and password are not passed in the XML request; however, they are part of the HTTP call.

If the authentication is unsuccessful, the *401 Unauthorized HTTP error* message appears.

You must use the ClearPass Policy Manager administrator credentials for authentication. If the administrator does not have the permissions to perform the read, write, and delete operations, the *401 Unauthorized HTTP error* message appears.

## Entity Names Supported

[Table 75](#) describes the **Entity Names** supported in the ClearPass Policy Manager Configuration API.

**Table 75:** Supported Entity Names in the Configuration API

Entity Name	Description
AdminPrivileges	Specifies the Admin user privileges.
AdminUser	Specifies the Admin user repository.
AuditPosture	Specifies the audit posture servers, such as Network Mapper (NMAP) and Nessus scanner.
AuthMethod	Specifies the authentication method to authenticate the user or device against an authentication source.
AuthSource	Specifies the identity store (Active Directory, LDAP Directory, SQL Database, and Token Server) against which users and devices are authenticated.
ContextServer	Specifies the Endpoint Context Server.
ContextServerAction	Specifies the Endpoint Context Server Actions dictionary to configure actions that are performed on endpoints.
DataFilter	Specifies the data filters used to filter records in Access Tracker and Syslog messages.
Endpoint	Specifies the Endpoint device details. <b>NOTE:</b> Profile information is not supported in the API.
EnforcementPolicy	Specifies the enforcement policy that applies conditions (roles, health, and time attributes) against specific values associated with those attributes to determine the enforcement profile.
EnforcementProfile	Specifies the enforcement profiles containing attributes that define a client's scope of access for the session.
ExtSyslog	Specifies the session data, audit records, and event records that can be sent to one or more syslog targets (servers).
GuestUser	Specifies the Guest accounts managed by the Guest module.
LocalUser	Specifies the Local User Repository.
NadClient	Specifies the network device.

Entity Name	Description
NadGroup	Specifies the network device group.
OnboardDevice	Specifies the Onboard devices managed by Onboard module.
PostureExternal	Specifies the External Posture Server.
PostureInternal	Specifies the Internal Posture Policy that tests requests against Internal Posture rules to assess device health.
ProxyTarget	Specifies the RADIUS request that needs to be proxied to another RADIUS server.
RADIUSDictionary	Specifies the RADIUS vendor attributes dictionary.
Role	Specifies a set of roles assigned by the role mapping policy.
RoleMapping	Specifies the Role-Mapping Policy.
ServerConfig	Provides the server configuration details. <b>NOTE:</b> Only the Read method is permitted.
Service	Specifies a service and its associated entities.
Simulation	Specifies the policy simulations that allow policies to be verified before they are deployed.
SnmpTrapConfig	Specifies SNMP trap receivers.
StaticHostList	Comprises of a list of MAC addresses and IP addresses. These can be used as white-lists or blacklists to control access to the network.
SyslogExportData	Specifies the Syslog Export Filters that notify Policy Manager where to send this information and what type of information should be sent through data filters.
TacacsServiceDictionary	Specifies the TACACS+ Service attributes dictionary.
TagDefinition	Specifies the Entity Tag Definitions.
TagDictionary	Specifies the Entity Tag Attributes dictionary.

## NameList

The **NameList** method returns the list of names for all objects created for an Entity type. The XML request contains an **EntityNameList** request passed in the entity-type. You can pass multiple **EntityNameList** requests for different Entity types.

In the XML response, **EntityNameList** is populated with the entity-names. The list of names in the XML response is not displayed in a specific order.

However, for the entities that have a specific order (for example, **Services**), the names are populated in the order as specified in the **EntityNameList**.

The URL for the **NameList** method is:

```
https://<server>/tipsapi/config/namelist/<Entity>
```

## XML Request

The following is an example of the **NameList** method XML request:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0"/>
<EntityNameList entity="Service"/>
</TipsApiRequest>
```

## XML Response

The following is an example of the **NameList** method XML response:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0"><TipsHeader
exportTime="Wed Aug 24 15:39:01 PST 2016" version="6.x"/>
<StatusCode>Success</StatusCode>
<EntityNameList entity="Service"><Name>[Policy Manager Admin Network Login Service]</Name><Name>[AirGroup Authorization Service]</Name><Name>[Aruba Device Access Service]</Name><Name>[Guest Operator Logins]</Name><Name>test 802.1X Wireless</Name>
</EntityNameList>
</TipsApiResponse>
```

## Reorder

The **Reorder** method receives a list of names of objects of the Entity type and applies the new order to the list of objects.

The XML request contains an **EntityOrderList** that should specify the Entity-type and a list of names. This list should contain the names of all elements of the Entity-type. The new order is returned in the XML response.

You can pass multiple **EntityOrderList** for different entity-types in the request. The Reorder method is available for the **Services** entity-type.

The URL for the **Reorder** method is:

```
https://<server>/tipsapi/config/reorder/<Entity>
```

## XML Request

The following is an example of the **Reorder** method XML request:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="6.x"/>
<EntityOrderList entity="Service"><Name>[Aruba Device Access Service]</Name>
<Name>[Guest Operator Logins]</Name><Name>test 802.1X Wireless</Name>
<Name>[Policy Manager Admin Network Login Service]</Name>
```

```
<Name>[AirGroup Authorization Service]</Name></EntityOrderList>
</TipsApiRequest>
```

## XML Response

The following is an example of the **Reorder** method XML response:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Wed Aug 24 15:45:24 PST 2016" version="6.x"/>
<StatusCode>Success</StatusCode>
<LogMessages><Message>Services have been reordered successfully</Message></LogMessages>
<EntityOrderList entity="Service"><Name>[Aruba Device Access Service]</Name>
<Name>[Guest Operator Logins]</Name><Name>test 802.1X Wireless</Name>
<Name>[Policy Manager Admin Network Login Service]</Name>
<Name>[AirGroup Authorization Service]</Name>
</EntityOrderList>
</TipsApiResponse>
```

## Status Change

The **Status Change** method gets the name-list of disabled and enabled entities of a specific type and changes the status of the entities as required. The XML request contains an **EntityStatusList** that includes the entity-type and a name-list.

You must specify the Enabled elements first and then the Disabled elements within the name-list. The status list of the entity is returned in the XML response.

Multiple **EntityStatusList** requests for different entity types are supported.

The URL for the **Status Change** method is:

*https://<server>/tipsapi/config/status/<Entity>*

## XML Request

The following is an example of the **Status Change** method XML request:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="6.x"/>
<EntityStatusList entity="Service">
<Enabled>[Aruba Device Access Service]</Enabled>
<Enabled>[Guest Operator Logins]</Enabled>
<Disabled>test 802.1X Wireless</Disabled>
<Disabled>[Policy Manager Admin Network Login Service]</Disabled>
</EntityStatusList>
</TipsApiRequest>
```

## XML Response

The following is an example of the **Status Change** method XML response:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Wed Aug 24 16:08:13 PST 2016" version="6.x"/>
<StatusCode>Success</StatusCode>
```

```

<LogMessages><Message>Status successfully changed</Message></LogMessages>
<EntityStatusList entity="Service">
<Enabled>[AirGroup Authorization Service]</Enabled>
<Enabled>[Aruba Device Access Service]</Enabled>
<Enabled>[Guest Operator Logins]</Enabled>
<Disabled>[Policy Manager Admin Network Login Service]</Disabled>
<Disabled>test 802.1X Wireless</Disabled>
</EntityStatusList>
</TipsApiResponse>

```

## ClearPass Configuration API Examples

This section contains the following information:

- [Introduction](#)
- [Using the Contains Match Operator](#)
- [Retrieving a Guest User Value](#)
- [Retrieving a Local User Value](#)
- [Adding a Guest User Value](#)
- [Updating a Guest User Value](#)
- [Removing a Guest User](#)

### Introduction

This section provides ClearPass Configuration API examples of XML requests and responses. With the examples provided in this section, you can retrieve, add, update, and remove the **Guest User** value and the **Local User** value.

### Using the Contains Match Operator

Use the **Contains** match operator to fetch more than one item.

For example, you could group Guest users who attend a conference in Rome using the format *Rome\_Conf\_<user\_name>*.

You can fetch the required group of Guest users using the criteria as described in the following example:

```

<Filter entity="GuestUser">
<Criteria fieldName="name" filterString=" Rome_Conf_" match="contains"/>
</Filter>

```

### Retrieving a Guest User Value

For the **GuestUser** and **OnboardDevice** entity types, you must use the source attribute with the value **Guest**. For other entity types, you do not need to include the source attribute.

Post the XML request to the following URL:

*https://<server>/tipsapi/config/read/GuestUser*

### XML Request

The following is an example of the XML request used to fetch all Guest users:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0" source="Guest"/>
<Filter entity="GuestUser"/>
</TipsApiRequest>
```

## Retrieving a Local User Value

For other entity types, you do not need to include the source attribute.

If the Guest description is present in the XML request, the GuestUserDetails element is displayed in the Guest details.

Post the XML request to the following URL:

*https://<server>/tipsapi/config/read/LocalUser*

## Fetching All Local Users

The following is an example of an XML request used to fetch all local users:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0"/>
<Filter entity="LocalUser"/>
</TipsApiRequest>
```

## Using Criteria in a Filter

The following is an example of using **Criteria** in a filter:

```
<Filter entity="GuestUser">
<Criteria fieldName="name" filterString="reynolds" match="equals"/>
</Filter>
```

## Retrieving a Specific Guest Name

The following is an example of the XML response that retrieves all Guest users with the name "reynolds."

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Wed Sep 24 10:47:26 PST 2016" version="6.x"/>
<StatusCode>Success</StatusCode>
<EntityMaxRecordCount>1</EntityMaxRecordCount>
<GuestUsers>
<GuestUser enabled="true" expiryTime="2016-12-29 12:24:37.0"
startTime="2016-09-29 12:26:08.28" sponsorName="admin" guestType="USER"
password="webco123#" name="reynolds">
<GuestUserDetails sendSms="false" sendEmail="true" description="Test"/>
<GuestUserTags tagName="Company Name" tagValue="WebCo"/>
<GuestUserTags tagName="Email Address" tagValue="reynolds@webco.net"/>
<GuestUserTags tagName="Location" tagValue="Room A"/>
</GuestUser>
</GuestUsers>
</TipsApiResponse>
```

## Adding a Guest User Value

For the Guest description, you must include the **GuestUserDetails** element as described in the following example.

You can set the **sendSms** and **sendEmail** attribute values to **false** as these values are not used by Guest.

### XML Request

Post the XML request to the following URL:

<https://<server>/tipsapi/config/write/<GuestUser>>

The following example of the XML request is similar to the XML response received in the Read method, except **StatusCodes**, **EntityMaxRecordCount**, and **exportTime** are omitted:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0" source="Guest"/>
<GuestUsers>
<GuestUser enabled="true" expiryTime="2016-12-30 12:24:37" startTime="2015-09-30 12:26:08"
sponsorName="admin" guestType="USER" password="webco123#" name="mike">
<GuestUserDetails sendSms="false" sendEmail="false" description="Test"/>
<GuestUserTags tagName="First Name" tagValue="Michael"/>
<GuestUserTags tagName="Email Address" tagValue="mike@webco.net"/>
<GuestUserTags tagName="Phone" tagValue="4888888888"/>
</GuestUser>
</GuestUsers>
</TipsApiRequest>
```

### XML Response

The following is an example of the XML response:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Wed Sep 28 10:51:27 PST 2016" version="3.0"/>
<StatusCode>Success</StatusCode>
<LogMessages>
<Message>Added 1 guest user(s)</Message>
</LogMessages>
</TipsApiResponse>
```

## Updating a Guest User Value

The **Write** method handles the **Update** operation and determines whether a passed object in the XML request is already present or not.

Depending on presence of the passed object, a new object is added or the existing object is updated.

Post the XML request to the following URL:

<https://<server>/tipsapi/config/write/<GuestUser>>

### XML Request

The following is an example of the XML request:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```

<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0" source="Guest"/>
<GuestUsers>
<GuestUser enabled="true" expiryTime="2016-09-18 12:24:37" startTime="2016-09-18 12:26:08"
sponsorName="admin" guestType="USER" password="webco123#" name="mike">
<GuestUserTags tagName="First Name" tagValue="Michael"/>
<GuestUserTags tagName="Last Name" tagValue="Penn"/>
<GuestUserTags tagName="Email Address" tagValue="mike@webco.net"/>
<GuestUserTags tagName="Phone" tagValue="4888888888"/>
</GuestUser>
</GuestUsers>
</TipsApiRequest>

```

## XML Response

The following is an example of the XML response:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Fri Sep 16 10:51:27 PST 2016" version="3.0"/>
<StatusCode>Success</StatusCode>
<LogMessages>
<Message>Updated 1 guest user(s)</Message>
</LogMessages>
</TipsApiResponse>

```

## Updated XML Response

The following is an example of the XML response with some objects added and updated:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Fri Sep 16 10:51:27 PST 2016" version="3.0"/>
<StatusCode>Success</StatusCode>
<LogMessages>
<Message>Added two guest user(s)</Message>
<Message>Updated three guest user(s)</Message>
</LogMessages>
</TipsApiResponse>

```

## Removing a Guest User

The **Remove** operation requires two steps, as illustrated in this example. To remove a Guest user with the name "reynolds," follow these steps.

### XML Request

- Post the XML request to the following URL:

```

https://<server>/tipsapi/config/deleteConfirm/<GuestUser>
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0" source="Guest"/>
<Filter entity="GuestUser">
<Criteria fieldName="name" filterString="reynolds" match="equals"/>

```

```
</Filter>
</TipsApiRequest>
```

## XML Response

The following is an example of the XML response:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Fri Sep 16 10:47:26 PST 2016" version="3.0"/>
<StatusCode>Success</StatusCode>
<EntityMaxRecordCount>1</EntityMaxRecordCount>
<GuestUsers>
<GuestUser enabled="true" expiryTime="2016-12-18 12:24:37.0"
startTime="2015-09-18 12:26:08.28" sponsorName="admin" guestType="USER"
password="webco123#" name="reynolds">
<element-id>GuestUser_reynolds_MCw</element-id>
<GuestUserTags tagName="Company Name" tagValue="Webco"/>
<GuestUserTags tagName="Email Address" tagValue="reynolds@webco.net"/>
<GuestUserTags tagName="Location" tagValue="Room A"/>
</GuestUser>
</GuestUsers>
</TipsApiResponse>
```

## XML Request

2. Extract the element-IDs and post the XML request to the following URL:

*<https://<server>/tipsapi/config/delete/<GuestUser>>*

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiRequest xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader version="3.0" source="Guest"/>
<Delete>
<Element-Id>GuestUser_reynolds_MCw</Element-Id>
</Delete>
</TipsApiRequest>
```

## XML Response

The following is an example of the XML response:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Fri Sep 16 10:56:00 PST 2016" version="3.0"/>
<StatusCode>Success</StatusCode>
<LogMessages>
<Message>Guest user deleted successfully</Message>
</LogMessages>
</TipsApiResponse>
```

# API Error Handling

This section contains the following information:

- [When There Is an Error During a Request](#)
- [InvalidFetchCriteria Example](#)

## When There Is an Error During a Request

When there is an error or failure during a request, the **StatusCode** is set to **Failure**. A **TipsApiError** element is set with an Error Code and a list of messages.



You must use the source attribute with the value **Guest** for the **GuestUser** and **OnboardDevice** entity types. For other entity types, you do not need to include the source attribute.

The following error codes are defined in the Admin API:

- **BadRequest**: Occurs when the method described in the following URL is not supported or is invalid:  
`https://<server>/tipsapi/config/<method>/<Entity>`
- **DependencyBreak**: Occurs when the Entity object is an element of some other Entity and is requested for deletion.
- **IllegalArgument**: Occurs when the Entity type is invalid or does not exist.
- **InvalidFetchCriteria**: Occurs when a specified field name does not exist for an entity type or the specified filter operation is invalid.
- **InvalidXml**: Occurs when XML has an invalid structure and contains some additional or missing elements.
- **ServiceFailure**: Occurs when an internal error is generated in API services.

## InvalidFetchCriteria Example

The following is an example of the error message that is generated when a specified field name does not exist for an entity type or the specified filter operation is invalid:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<TipsApiResponse xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
<TipsHeader exportTime="Wed May 25 15:31:41 PST 2016" version="6.6"/>
<StatusCode>Failure</StatusCode>
<TipsApiError>
<ErrorCode>InvalidFetchCriteria</ErrorCode>
<Message>Invalid FieldName. 'macaddress' is not a field of Endpoint entity</Message>
</TipsApiError>
</TipsApiResponse>
```

## About the API Explorer

In addition to the ClearPass Configuration API, Aruba offers a number of other APIs that are available through the API Explorer:

**Table 76: ClearPass APIs Available Through the API Explorer**

API	Services Provided
ApiFramework	ApiClient
GuestManager	Configuration, Device, Guest
Onboard	Certificate, CertificateChain, CertificateExport, CertificateImport, CertificateNew, CertificateReject, CertificateRequest, CertificateRevoke, CertificateSign
OperatorLogins	GetAccount, GetPrivileges
Platform	ClusterDbSync
SmsServices	SmsSend

To access the API Explorer:

1. Log into the ClearPass Policy Manager server and select **ClearPass Guest** from **Applications** or **Quick Links**.
2. In ClearPass Guest, navigate to **Administration > API Services > API Clients**.  
The API Clients page opens.

**Figure 210 API Clients Page**

The API clients you have defined are listed below.

Client ID	Grant Types	Access Token	Operator Profile
client_credentials	client_credentials	8 hours	IT Administrators
Guest API Testing	password refresh_token	8 hours	IT Administrators
username_password	password refresh_token	8 hours	IT Administrators

3. Click the **API Explorer** link.

The API Explorer dialog opens.

**Figure 211 API Explorer Dialog**

## API Explorer

API	Services	Versions
ApiFramework	ApiClient	v1
GuestManager	Configuration, Device, Guest	v1
Onboard	Certificate, CertificateChain, CertificateExport, CertificateImport, CertificateNew, CertificateReject, CertificateRequest, CertificateRevoke, CertificateSign	v1
OperatorLogins	GetAccount, GetPrivileges	v1
Platform	ClusterDbSync	v1
SmsServices	SmsSend	v1

4. Select the API of choice.

The API page for the selected API opens. The example in [Figure 212](#) is the OperatorLogins API.

**Figure 212 OperatorLogins API Selected**

## API Explorer – OperatorLogins-v1

[Back to API Explorer](#)

**Authorization:** Enter Authorization header value here

**GetAccount : Returns user account information**

[Show/Hide](#) | [List Operations](#) | [Expand Operations](#)

**GET** /oauth/me

Returns user account information

**POST** /oauth/me

Returns user account information

**GetPrivileges : Determine the privileges available to the user**

[Show/Hide](#) | [List Operations](#) | [Expand Operations](#)

5. In the **Authorization** field, enter the **Authorization header value**.

6. Proceed to work in the API as needed.

7. To return to the API Explorer, click **Back to API Explorer**.