



**Dell Networking
W-ClearPass
Deployment Guide**

Copyright

© Copyright 2016 Hewlett Packard Enterprise Development LP. Dell™, the DELL™ logo, and PowerConnect™ are trademarks of Dell Inc.

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. You may request a copy of this source code free of charge at HPE-Aruba-gplquery@hpe.com. Please specify the product and version for which you are requesting source code.

Contents

Copyright	2
Contents	3
About W-ClearPass	11
About This Guide	11
Intended Audience	11
About the W-ClearPass Access Management System	12
W-ClearPass Access Management System Overview	12
Key Features	13
Advanced Policy Management	13
W-ClearPass Policy Manager Hardware and Virtual Appliances	14
W-ClearPass Specifications	14
Setting Up the W-ClearPass Hardware Appliances	15
About the W-ClearPass Hardware Appliances	16
W-ClearPass Policy Manager 500 Hardware Appliance	16
W-ClearPass Policy Manager 5K Hardware Appliance	18
W-ClearPass Policy Manager 25K Hardware Appliance	19
Before Starting the W-ClearPass Installation	21
Configuring the W-ClearPass Hardware Appliance	22
Activating W-ClearPass	23
Logging in to the W-ClearPass Hardware Appliance	24
Signing Up for Live Software Updates	25
Changing the Administration Password	25
Powering Off the W-ClearPass Hardware Appliance	26
Resetting the System Passwords to the Factory Defaults	27
Using the VMware vSphere Web Client to Install W-ClearPass on a Virtual Machine	28
Introduction	28
Before Starting the W-ClearPass Installation	29

vSphere Web Client W-ClearPass Installation Overview	30
W-ClearPass VMware Virtual Appliance Installation Setup	30
Adding a Virtual Hard Disk	33
Launching the W-ClearPass Virtual Appliance	35
Completing the Virtual Appliance Setup	36
Applying and Activating the W-ClearPass License	37
Logging in to the W-ClearPass Virtual Appliance	39
Signing Up for Live Software Updates	40
Changing the Administration Password	40
Powering Off the W-ClearPass Virtual Appliance	41
Using Microsoft Hyper-V to Install W-ClearPass on a Virtual Appliance	41
Introduction	42
Before Starting the W-ClearPass Installation	43
W-ClearPass Hyper-V Virtual Appliance Installation Summary	44
Importing the Virtual Machine	44
Adding a Hard Disk to a Virtual Machine	48
Launching the W-ClearPass Virtual Appliance	51
Completing the Virtual Appliance Configuration	53
Applying and Activating the W-ClearPass License	54
Logging in to the W-ClearPass Virtual Appliance	55
Signing Up for Live Software Updates	56
Changing the Administration Password	56
Powering Off the W-ClearPass Virtual Appliance	57
Accessing the W-ClearPass Administrative Interface	57
Supported Browsers	58
Accessing the Administrative Interface	58
Changing the Administration Password	59
Accessing W-ClearPass Online Help	60
Maintaining W-ClearPass Policy Manager Services	60

Starting or Stopping W-ClearPass Services	60
Summary of the Server Configuration Page	61
Subset of CLI for W-ClearPass Maintenance Tasks	62
Preparing the Mobility Controller for W-ClearPass Policy Manager Integration	65
Adding a Mobility Controller to W-ClearPass Policy Manager	65
Defining a New Mobility Controller	65
Importing a List of Network Devices	67
Generating an Example of Import File XML Format	67
Adding a W-ClearPass/RADIUS Server to the Mobility Controller	68
Adding the W-ClearPass/RADIUS Server to a Server Group	73
Configuring an AAA Profile for 802.1X Authentication	75
Configuring a Virtual AP Profile	79
About Virtual AP Profiles	79
Configuring the Virtual AP Profile	80
Configuring W-ClearPass as an RFC 3576 (CoA) Server	83
About the CoA Server	84
Configuring the W-ClearPass Server as a CoA Server	84
Using the CLI	85
Adding an SSID to the Mobility Controller for 802.1X Authentication	85
SSID Profile Overview	85
Adding an SSID to the Mobility Controller	86
Preparing for Active Directory Authentication	93
Joining a W-ClearPass Server to an Active Directory Domain	93
Introduction	93
Confirming the Date and Time Are in Sync	94
Joining an Active Directory Domain	95
About the Authentication Source and the Authorization Process	98
Manually Specifying Active Directory Domain Controllers for Authentication	98
Disassociating a W-ClearPass Server From an Active Directory Domain	99

Adding Active Directory as an Authentication Source to W-ClearPass	100
About Authorization	101
User Objects	101
About the Bind Operation	101
Adding Active Directory as an Authentication Source	101
Obtaining and Installing a Signed Certificate From Active Directory	108
About Certificates in W-ClearPass Deployments	108
How to Obtain a Signed Certificate from Active Directory	109
Creating a Certificate Signing Request	109
Importing the Root CA Files to the Certificate Trust List	112
Obtaining a Signed Certificate from Active Directory	113
Importing a Server Certificate into W-ClearPass	117
Manually Testing Login Credentials Against Active Directory	118
Preparing for 802.1X Wireless Authentication with Active Directory	119
About 802.1X Authentication	119
Introducing 802.1X	119
802.1X Authentication Components	119
What Is AAA?	121
Authentication	121
Authorization	121
Accounting	121
Configuring 802.1X Wireless Authentication with Active Directory	121
Authenticating Against Active Directory	122
About the 802.1X Wireless Service	122
Creating the 802.1X Wireless Service	123
Deleting a W-ClearPass Policy Manager Service	127
Walking Through an 802.1X Authentication Scenario	128
802.1X Wireless Authentication Traffic Flow	128
Walking Through the 802.1X Authentication Process	128

802.1X Wired Authentication Traffic Flow	129
Troubleshooting 802.1X Configuration Issues	129
Active Directory Authentication Source Configuration Issues	129
Mobility Controller Configuration Issues	129
Deploying W-ClearPass Clusters	131
W-ClearPass Cluster Overview	131
Introduction	131
W-ClearPass Databases	132
Publisher/Subscriber Model	132
Network Ports That Must Be Enabled	134
Cluster Scaling Limitations	135
Cluster Design Considerations	135
Cluster Deployment Sizing Guidance	135
Publisher Node Guidelines	136
Subscriber Node Guidelines	137
Providing Sufficient Bandwidth Between Publisher and Subscribers	138
RTT Considerations When Building Geographically Distributed Clusters	138
Implementing W-ClearPass Zones for Geographical Regions	139
About Large Scale Deployments	141
What Is a Large Scale Deployment?	141
Design Guidelines	141
Examples of Customer Cluster Deployments	142
Deploying the Standby Publisher	144
Setting Up the Standby Publisher	144
About the Fail-Over Process	145
Mitigation Strategies	145
Virtual IP Address Considerations	146
Functions Lost When the Publisher Is Down	146
Adding a Subscriber Node to the Publisher	146

Introduction	146
Using the WebUI to Add a Subscriber Node	147
Using the CLI to Create a Subscriber Node	149
Rejoining a Down Node to the Cluster	150
Introduction	150
Removing a Subscriber Node from the Cluster	150
Rejoining a Node Back Into the Cluster	151
Deploying W-ClearPass Insight in a Cluster	152
Introduction	152
W-ClearPass Insight Placement Considerations	153
When a W-ClearPass Insight-Enabled Node Is Down	153
Enabling W-ClearPass Insight	153
Configuring Cluster File-Backup Servers	154
Adding Cluster File-Backup Servers	154
Backing Up Configuration and Access Tracker Log Information	156
Using High Capacity Guest Mode	157
Introduction	158
Licensing Considerations	158
EAP-PSK Protocol	159
Enabling High Capacity Guest Mode	159
Cleanup Intervals Settings for High Capacity Guest Mode	160
Service Templates Supported	161
Service Types Supported	161
Authentication Methods Supported	161
Cluster CLI Commands	162
cluster drop-subscriber	162
cluster list	162
cluster make-publisher	163
cluster make-subscriber	163

cluster reset-database	164
cluster set-cluster-passwd	164
cluster sync-cluster-passwd	164
Mobility Access Switch Configuration for 802.1X Authentication	165
Mobility Access Switch Configuration for 802.1X Wired Authentication	165
About Defining Wired 802.1X Authentication	165
Configuring Authentication with a RADIUS Server	166
Authentication Terminated on the Mobility Access Switch	167
Configuring Access Control Lists	168
CLI-Based Configuration for Mobility Access Switch 802.1X Authentication	169
Termination Options	169
Configuring a Server Rule Using the CLI	171
Setting Variables for LDAP Servers	171
Configuring Certificates with Authentication Termination	171
Configuring 802.1X Authentication with Machine Authentication	172
About Machine Authentication	172
Enabling the Enforce Machine Authentication Option	172
Role Assignment with Machine Authentication Enabled	173
VLAN Assignments	174
Authentication with an 802.1x RADIUS Server	175
Examples of Common 802.1X Configuration Tasks Via the CLI	176
Preparing W-ClearPass for LDAP and SQL Authentication Sources	179
LDAP Authentication Source Configuration	179
Configuring Generic LDAP Authentication Sources	179
SQL Authentication Source Configuration	184
Configuring a Generic SQL Authentication Source	184
Defining a Filter Query	188
802.1X EAP-PEAP Reference	191
A Tour of the EAP-PEAP-MSCHAPv2 Ladder	191

About EAP-PEAP MSCHAPv2	191
EAP-PEAP MSCHAPv2 Handshake Exchange Summary	191
Using the W-ClearPass Configuration API	199
W-ClearPass Configuration API Overview	199
Introduction	199
Admin Accounts for API Access	199
XML Data Structure	200
Filter Elements	201
Advanced Match Operations	201
Setting Up Bulk Access for Endpoints and Guest Accounts	202
W-ClearPass Configuration API Methods	204
Introduction	204
Authentication Credentials	204
Entity Names Supported	205
NameList	206
Reorder	207
Status Change	208
W-ClearPass Configuration API Examples	209
Introduction	209
Using the Contains Match Operator	209
Retrieving a Guest User Value	209
Retrieving a Local User Value	210
Adding a Guest User Value	211
Updating a Guest User Value	211
Removing a Guest User	212
API Error Handling	214
When There Is an Error During a Request	214
InvalidFetchCriteria Example	214
About the API Explorer	215

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

This chapter includes the following information:

- [About This Guide](#)
- [About the W-ClearPass Access Management System](#)
- [Setting Up the W-ClearPass Hardware Appliances](#)
- [Using the VMware vSphere Web Client to Install W-ClearPass on a Virtual Machine](#)
- [Using Microsoft Hyper-V to Install W-ClearPass on a Virtual Appliance](#)
- [Maintaining W-ClearPass Policy Manager Services](#)

About This Guide

Welcome to the *W-ClearPass 6.6 Deployment Guide*.

The *W-ClearPass 6.6 Deployment Guide* is intended to assist field System Engineers and network administrators, as well as customers and partners, in deploying W-ClearPass Policy Manager.

This guide is organized in a way that presents the recommended sequence in which W-ClearPass deployment should take place, and makes the major deployment tasks easy to understand and implement.

The *W-ClearPass 6.6 Deployment Guide* includes the following information:

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

Intended Audience

The intended audience for the *W-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 W-ClearPass Essentials and, if possible, Dell Certified W-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
- User Identity stores, such as Active Directory



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 W-ClearPass Access Management System

This section contains the following information:

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

W-ClearPass Access Management System Overview

The Dell W-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 W-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 W-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.

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

Self-Service Capabilities

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

W-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

W-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

W-ClearPass's key features are as follows:

- Role-based network access enforcement for multivendor Wi-Fi, wired, and VPN networks
- High performance, scalability, High Availability, and load balancing
- A Web-based user interface that simplifies policy configuration and troubleshooting
- Network Access Control (NAC), Network Access Protection (NAP) posture and health checks, and Mobile Device Management (MDM) integration for mobile device posture checks
- Auto Sign-On and single sign-on (SSO) support via Security Assertion Markup Language (SAML) v2.0
- Social Network and Cloud Application SSO via OAuth2
 - Facebook, Twitter, LinkedIn, Office365, Google Apps, and so on
- Built-in Bring Your Own Device (BYOD) Certificate Authority for secure self-service onboarding
- 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

W-ClearPass advanced policy management support includes:

- **Employee access**

W-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**

W-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, W-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**

W-ClearPass Onboard fully automates the provisioning of any Windows, Mac OS X, iOS, Android, Chromebook, and Ubuntu devices via a built-in captive portal. Valid users are redirected to a template-based interface to configure required SSIDs and 802.1X settings, and download unique device credentials. Additional capabilities include the ability for IT to revoke and delete credentials for lost or stolen devices, and the ability to configure mobile email settings for Exchange ActiveSync and VPN clients on some device types.

- **Customizable visitor management**

W-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**

W-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, anti-spyware, firewall, and peer-to-peer applications) to enhance authorization policies. Automatic remediation services are also available for non-compliant devices.

W-ClearPass Policy Manager Hardware and Virtual Appliances

W-ClearPass Policy Manager is available as hardware or a virtual appliance that supports 500, 5000, and 25,000 authenticating devices.

- For hardware virtual appliance installation and deployment procedures, see [Setting Up the W-ClearPass Hardware Appliances on page 15](#)

Virtual appliances are supported on two platforms:

- VMware ESX and ESXi

For installation and deployment procedures, see [Using the VMware vSphere Web Client to Install W-ClearPass on a Virtual Machine on page 28](#).

- Microsoft Hyper-V

For installation and deployment procedures, see [Using Microsoft Hyper-V to Install W-ClearPass on a Virtual Appliance on page 41](#).

To increase scalability and redundancy, you can deploy virtual appliances, as well as the hardware appliances, within a cluster.

W-ClearPass Specifications

W-ClearPass Policy Manager

- Comprehensive identity-based policy engine
- Posture agents for Windows, Mac OS X, and Linux operating systems
- Built-in AAA services: RADIUS, TACACS+, and Kerberos
- Web, 802.1X, and non-802.1X authentication and authorization

- Reporting, analytics, and troubleshooting tools
- External captive portal redirect to multivendor equipment
- Interactive policy simulation and monitor mode utilities
- Deployment templates for any network type, identity store, and endpoint

Framework and Protocol Support

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

Supported Identity Stores

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

Setting Up the W-ClearPass Hardware Appliances

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

This section contains the following information:

- [About the W-ClearPass Hardware Appliances](#)
- [W-ClearPass Policy Manager 500 Hardware Appliance](#)
- [W-ClearPass Policy Manager 5K Hardware Appliance](#)
- [W-ClearPass Policy Manager 25K Hardware Appliance](#)
- [Before Starting the W-ClearPass Installation](#)
- [Configuring the W-ClearPass Hardware Appliance](#)
- [Activating W-ClearPass](#)
- [Logging in to the W-ClearPass Hardware Appliance](#)
- [Signing Up for Live Software Updates](#)
- [Powering Off the W-ClearPass Hardware Appliance](#)

- [Resetting the System Passwords to the Factory Defaults](#)

About the W-ClearPass Hardware Appliances

Dell provides three hardware appliance platforms:

- W-ClearPass Policy Manager 500
See [W-ClearPass Policy Manager 500 Hardware Appliance](#)
- W-ClearPass Policy Manager 5K
See [W-ClearPass Policy Manager 5K Hardware Appliance](#).
- W-ClearPass Policy Manager 25K
See [W-ClearPass Policy Manager 25K Hardware Appliance](#).

Table 1: *Functional Description of the W-ClearPass Hardware Appliance Ports*

Port	Description
Serial port	The Serial port is used to initially configure the W-ClearPass hardware appliance using a hard-wired terminal.
VGA connector	You can use the VGA Connector to connect the W-ClearPass hardware appliance to a monitor and keyboard.
USB ports	Two USB v2.0 ports are provided.
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.
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.
iDRAC7 Enterprise port	Provides remote access to the system—whether or not there is a functioning operating system running on the appliance. Allows administrators to monitor, manage, update, troubleshoot, and remediate the W-ClearPass 25K appliance from any location. NOTE: Available only on the CP-HW-25K appliance.

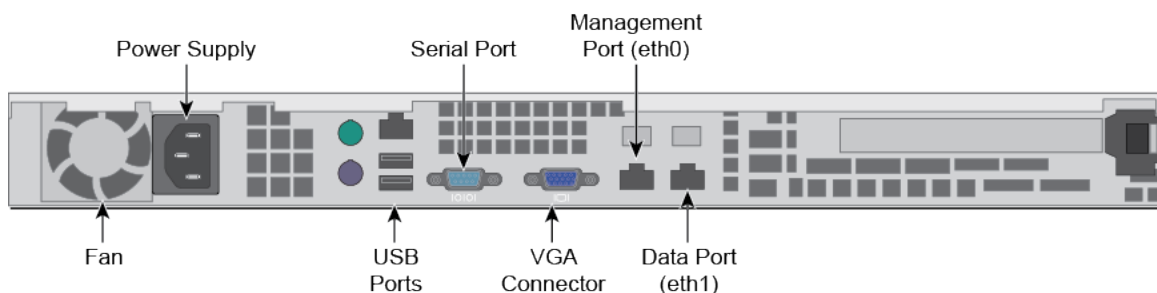
W-ClearPass Policy Manager 500 Hardware Appliance

The W-ClearPass Policy Manager 500 hardware appliance (CP-HW-500) is a RADIUS/ TACACS+ server that provides advanced policy control for up to 500 unique endpoints.

CP-HW-500 has a single 500GB SATA disk with no RAID disk protection.

[Figure 1](#) shows the ports on the rear panel of the W-ClearPass 500 hardware appliance. The function of each of these ports is described in [Table 1](#).

Figure 1 Ports on the W-ClearPass 500 Hardware Appliance



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

[Table 2](#) describes the specifications for the W-ClearPassPolicy Manager 500 hardware appliance.

Table 2: CP-HW-500 Specifications

CP-HW-500 Component	Specification
CPU	Pentium G850, Dual Core, 2.9Ghz, 3MB Cache
Memory	4 GB (2 x2GB)
Hard drive storage	500GB 7.3K RPM, Serial ATA
Maximum unique endpoints	<ul style="list-style-type: none"> High Capacity Guest (HGC) mode enabled: 1,000 HGC not enabled: 500
Maximum number of authentications per day	<ul style="list-style-type: none"> High Capacity Guest (HGC) mode enabled: 40,000 HGC not enabled: 20,000
Form Factor	
Dimensions (WxHxD)	16.8" x 1.7" x 14"
Weight (max configuration)	14 lbs
Power Specifications	
Power consumption (maximum)	260 watts
Power supply	Single
AC input voltage	100/240 VAC auto-selecting
AC input frequency	50/60 Hz auto-selecting

CP-HW-500 Component	Specification
Environmental Specifications	
Operating temperature	10° C to 35° C (50° F to 95° F)
Operating vibration	0.26 G at 5 Hz to 350 Hz for 5 minutes
Operating shock	1 shock pulse of 31 G for up to 2.6 ms
Operating altitude	-16 m to 3,048 m (-50 ft to 10,000 ft)

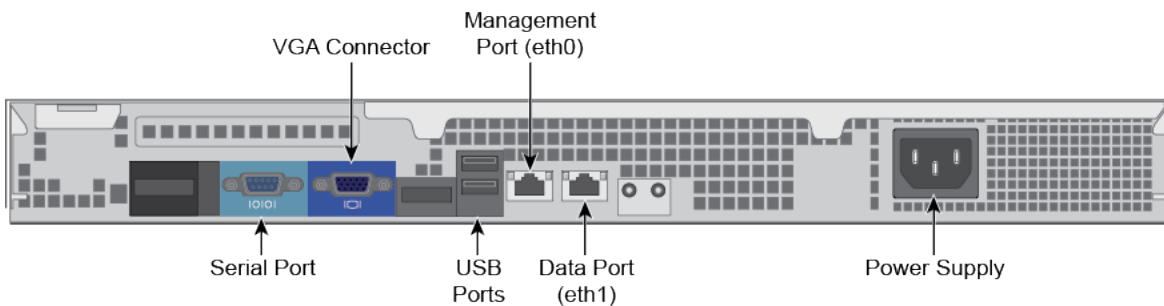
W-ClearPass Policy Manager 5K Hardware Appliance

The W-ClearPass Policy Manager 5K hardware appliance (CP-HW-5K) is a RADIUS/ TACACS+ server that provides advanced policy control for up to 5,000 unique endpoints.

CP-HW-5K ships with two x 1TB SATA disk drives. These drives are managed by an LSI RAID controller. The drives are configured as a RAID1 pair (RAID1 = block level mirroring). The LSI controller presents to W-ClearPass a single virtual 1TB drive, masking the two underlying physical drives.

[Figure 2](#) shows the ports on the rear panel of the W-ClearPass 5K hardware appliance. The function of each of these ports is described in [Table 1](#).

Figure 2 Ports on the W-ClearPass 5K Hardware Appliance



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

[Table 3](#) describes the specifications for the W-ClearPass Policy Manager 5K hardware appliance.

Table 3: CP-HW-5K Specifications

CP-HW- 5K Component	Specification
CPU	Xeon E3-1220 3.10 GHz, 8M Cache, Quad Core/4T
Memory	8GB Memory (4x2GB)
Hard disks	(2) 1TB 7.2K RPM SATA 3Gbps

CP-HW- 5K Component	Specification
<ul style="list-style-type: none"> RAID controller RAID configuration 	<ul style="list-style-type: none"> PERC H200 1
OOB management	Baseboard Management Controller (BMC)
Maximum unique endpoints	<ul style="list-style-type: none"> High Capacity Guest (HGC) mode enabled: 10,000 HGC not enabled: 5,000
Maximum number of authentications per day	<ul style="list-style-type: none"> High Capacity Guest (HGC) mode enabled: 400,000 HGC not enabled: 200,000
Form Factor	
Dimensions (WxHxD)	17.53" x 1.7" x 16.8"
Weight (max configuration)	18 lbs
Power Specifications	
Power consumption (maximum)	250 watts
Power supply	Single
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)
Operating vibration	0.26 G at 5 Hz to 350 Hz for 5 minutes
Operating shock	1 shock pulse of 31 G for up to 2.6 ms
Operating altitude	-16 m to 3,048 m (-50 ft to 10,000 ft)

W-ClearPass Policy Manager 25K Hardware Appliance

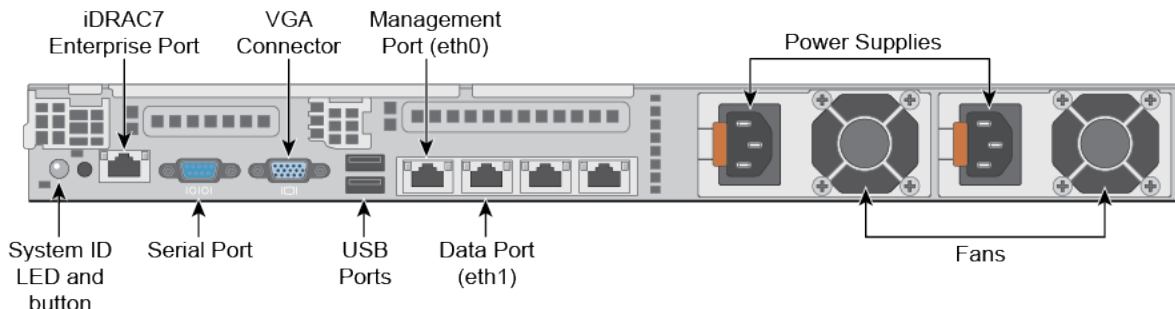
The W-ClearPass Policy Manager 25K hardware appliance (CP-HW-25K) is a RADIUS/ TACACS+ server that provides advanced policy control for up to 25,000 unique endpoints.

CP-HW-25K ships with four 300GB 10K Serial-Attach SCSI (SAS) disk drives. These drives are managed by a Dell Power Edge Raid Controller (PERC). The disk drives are configured as a RAID10 group.

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

[Figure 3](#) shows the ports on the rear panel of the W-ClearPass 25K hardware appliance. The function of each of these ports is described in [Table 1](#).

Figure 3 Ports on the W-ClearPass 25K Hardware Appliance



[Table 4](#) describes the specifications for the W-ClearPass Policy Manager 25K hardware appliance.

Table 4: CP-HW-25K Specifications

CP-HW-25K Component	Specification
CPUs	(2) Xeon X5650 2.66Ghz, 12M Cache, Turbo, HT
Memory	48GB Memory (12x4GB)
Hard disks	(4) 300GB 10K RPM Serial-Attach SCSI 6Gbps
Maximum unique endpoints	<ul style="list-style-type: none"> High Capacity Guest (HGC) mode enabled: 50,000 HGC not enabled: 25,000
Maximum number of authentications per day	<ul style="list-style-type: none"> High Capacity Guest (HGC) mode enabled: 2 million HGC not enabled: 1 million
<ul style="list-style-type: none"> RAID controller RAID configuration 	<ul style="list-style-type: none"> PERC 6/i 10
OOB management	iDRAC7 Enterprise
Form Factor	
Dimensions (WxHxD)	16.8" x 1.7" x 27.8"
Weight (max configuration)	Up to 39 lbs
Power Specifications	

CP-HW-25K Component	Specification
Power consumption (maximum)	750 watts
Power supply	Dual hot-swappable (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)
Operating vibration	0.26 G at 5 Hz to 350 Hz for 5 minutes
Operating shock	1 shock pulse of 31 G for up to 2.6 ms
Operating altitude	-16 m to 3,048 m (-50 ft to 10,000 ft)

Before Starting the W-ClearPass Installation

Before starting the W-ClearPass installation and configuration procedures for the hardware appliance, determine the following information for the W-ClearPass server on your network, note the corresponding values for the parameters listed in [Table 5](#), and keep it for your records:

Table 5: W-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)	NOTE: Make sure that the Data port IP address is <i>not</i> in the same subnet as the Management port IP address.

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

Configuring the W-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 W-ClearPass hardware appliance.

To configure the W-ClearPass Policy Manager hardware appliance:

1. Connect the Serial port.

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

The hardware appliance is now available for configuration.

2. Configure the Serial port.

Apply the following parameters for 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 W-ClearPass hardware appliance.

Follow the prompts, replacing the placeholder entries in the following illustration with the information you entered in [Table 5](#):

- 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 25](#)

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

Activating W-ClearPass

To activate W-ClearPass Policy Manager and apply the W-ClearPass license:

- After the configuration has been applied at the virtual appliance console, open a web browser and go to the management interface of W-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 W-ClearPass server in [Table 5](#).
- Accept any security warnings from your browser regarding the self-signed SSL certificate, which comes installed in W-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 4 *Activating W-ClearPass*

You have 90 day(s) to activate the product

[Activate Now](#)

The screenshot shows a web form titled "Admin Login". It has a dark blue header with the text "Admin Login" in white. Below the header, there are two input fields: "Username:" and "Password:". At the bottom of the form, there is a blue button labeled "Log In".

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

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

If the W-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 5](#).

Figure 5 *Performing Offline Activation*

The screenshot shows a web interface for product activation. At the top, a red banner reads "You have 90 day(s) to activate the product". Below this, there are three main sections: "Online Activation" with an "Activate Now" button; "Offline Activation" which includes instructions and three steps: 1. Download an Activation Request Token (with a "Download" button), 2. Email the Activation Request Token to Aruba Networks Support (support@arubanetworks.com), and 3. Upload the Activation Key received from Aruba Networks Support (with a "Choose File" button and "no file selected" text, and an "Upload" button); and "Update License" with an "Update License" button.

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

Logging in to the W-ClearPass Hardware Appliance

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

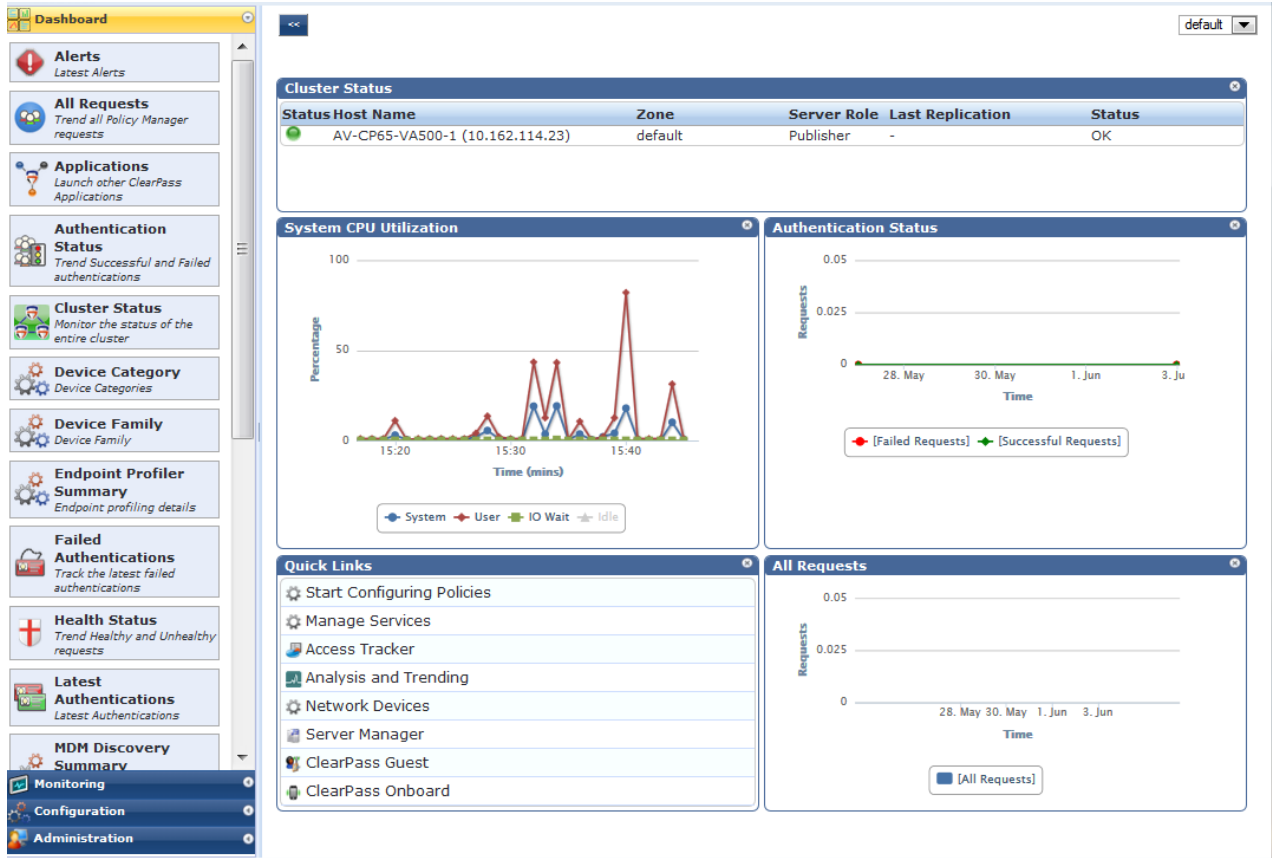
Figure 6 *Logging in to the W-ClearPass Hardware Appliance*

The screenshot shows the "Admin Login" dialog box. It has a title bar "Admin Login" and two input fields: "Username:" with the text "admin" and "Password:" with masked characters ".....". Below the fields is a "Log In" button.

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

The W-ClearPass Policy Manager Landing Page opens.

Figure 7 W-ClearPass Policy Manager Landing Page



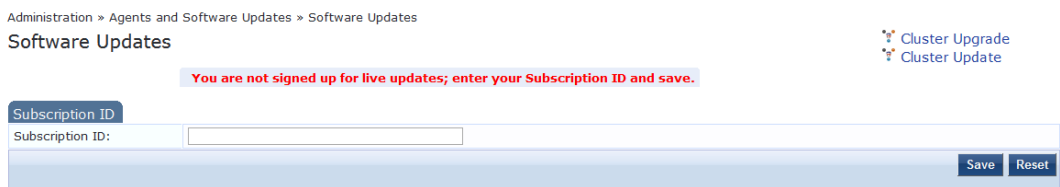
Signing Up for Live Software Updates

Upon your initial login to W-ClearPass Policy Manager, you should register for software updates.

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

A message is displayed indicating that the W-ClearPass hardware appliance is not signed up for live updates and that you must enter your subscription ID.

Figure 8 Entering the Subscription ID for Live Updates



2. If the W-ClearPass Policy Manager has Internet access, enter your subscription ID, then click **Save**.

After successfully applying the subscription ID, you will see a message indicating that the subscription ID was updated successfully and W-ClearPass is processing updates from the W-ClearPass Webservice.

Note that Posture & Profile Data Updates are downloaded and installed automatically, while Firmware & Patch Updates are display only.

Changing the Administration Password

When the cluster password for this W-ClearPass server is set upon initial configuration, the administration password is also set to the same password (see [Configuring the W-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 W-ClearPass, navigate to **Administration > Users and Privileges > Admin Users**.

The **Admin Users** page appears.

Figure 9 Admin Users Page

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

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

The **Edit Admin User** dialog appears.

Figure 10 Changing the Administration Password

User ID:	admin
Name:	Super Admin
Password:
Verify Password:
Privilege Level	Super Administrator

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

Powering Off the W-ClearPass Hardware Appliance

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

To power off the W-ClearPass hardware appliance:

1. Connect to the CLI from the serial console using the serial port.
2. Enter the following commands:
 - login: poweroff
 - password: poweroff

The W-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 W-ClearPass Policy Manager hardware appliance using the serial port (using any terminal program). See [Configuring the W-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 Dell 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 Dell 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**.
4. You can now log in with the new administrator password emailed to you by Dell Technical Support.

Using the VMware vSphere Web Client to Install W-ClearPass on a Virtual Machine

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

This section contains the following information:

- [Introduction](#)
- [Before Starting the W-ClearPass Installation](#)
- [vSphere Web Client W-ClearPass Installation Overview](#)
- [W-ClearPass VMware Virtual Appliance Installation Setup](#)
- [Adding a Virtual Hard Disk](#)
- [Launching the W-ClearPass Virtual Appliance](#)
- [Completing the Virtual Appliance Setup](#)
- [Applying and Activating the W-ClearPass License](#)
- [Logging in to the W-ClearPass Virtual Appliance](#)
- [Signing Up for Live Software Updates](#)
- [Changing the Administration Password](#)
- [Powering Off the W-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 ESX/ESXi 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 W-ClearPass Policy Manager 6.x installations.

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

W-ClearPass VMware ships with a 20 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 33](#) for details). The additional space required depends on the W-ClearPass virtual appliance version.

Processing and Memory Requirements

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

W-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. W-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 appropriate version of the W-ClearPass Release Notes at <https://download.dell-pcw.com> under the W-ClearPass 6.6.0 Upgrade folder. Access to this site requires log-in credentials.

Supported Hypervisors

W-ClearPass supports the following hypervisors:

- VMware ESX 4.0
Recommended minimum version for CP-VA-500 and CP-VA-5K.
VMware ESX 4.0 does not support greater than the eight virtual CPUs required for the CP-VA-25K.
- VMware ESXi versions 5.0, 5.1, 5.5, 6.0, and higher

Before Starting the W-ClearPass Installation

Before starting the W-ClearPass installation and configuration procedures for the virtual appliance, determine the following W-ClearPass server information on your network, note the corresponding values for the parameters listed in [Table 6](#), and keep it for your records:

Table 6: *W-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)	NOTE: 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)	

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

vSphere Web Client W-ClearPass Installation Overview

W-ClearPass VMware software packages are distributed as Zip files.

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

- 1.
1. Download the VMware ESXi package from the from the Dell Download site at <http://download.dell-pcw.com> to a folder accessible by your VMware ESXi server.
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.

W-ClearPass VMware Virtual Appliance Installation Setup

To set up the W-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 W-ClearPass that you want to install as a virtual appliance.



W-ClearPass Release Notes are available at <https://download.dell-pcw.com> under the W-ClearPass 6.6 Upgrade folder. Access to this site requires log-in credentials

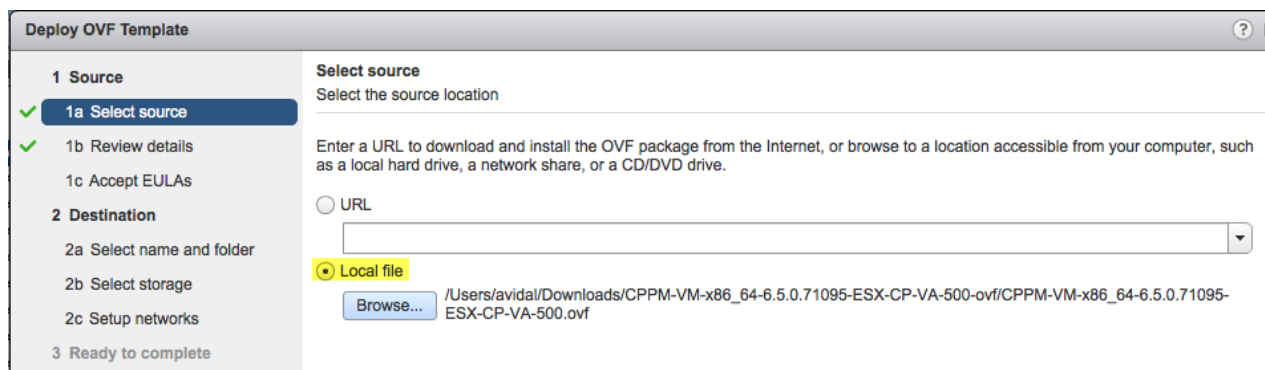
2. Then check the recommended virtual hardware specifications and verify that your system meets those requirements.
3. Start the VMware vSphere Web Client.
4. Extract the files into a folder on your desktop.
5. Using either the VMware vSphere Web Client or the standard vSphere Client, deploy the Open Virtualization Format (OVF) template that was downloaded and extracted in **Steps 3 and 4**.

The Deploy OVF Template opens.



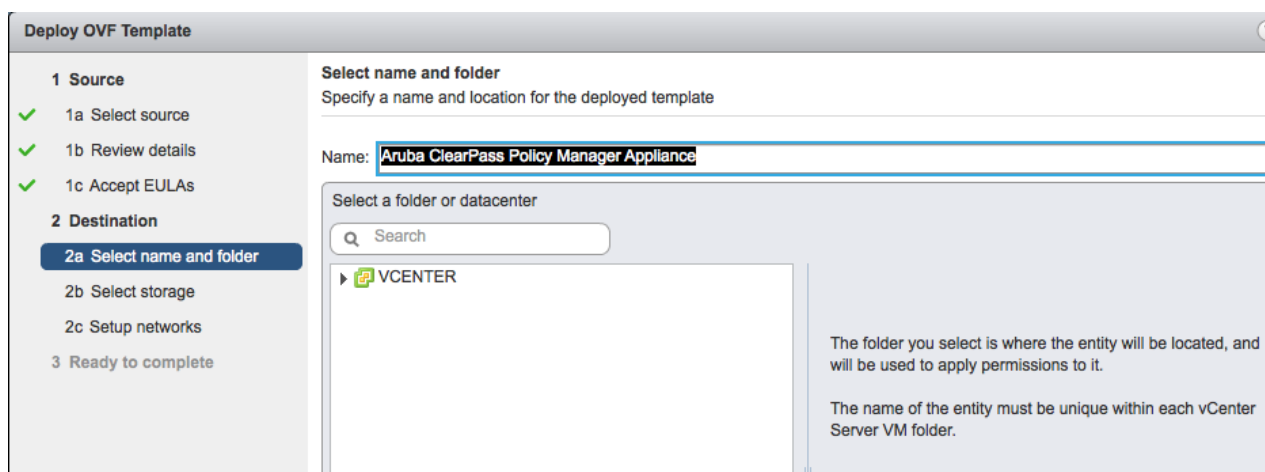
If you are not using the vSphere Web Client or the standard vSphere Client, follow the instructions for your method of deploying the OVF file.

Figure 11 *Deploy OVF Template: Selecting the Source Location*



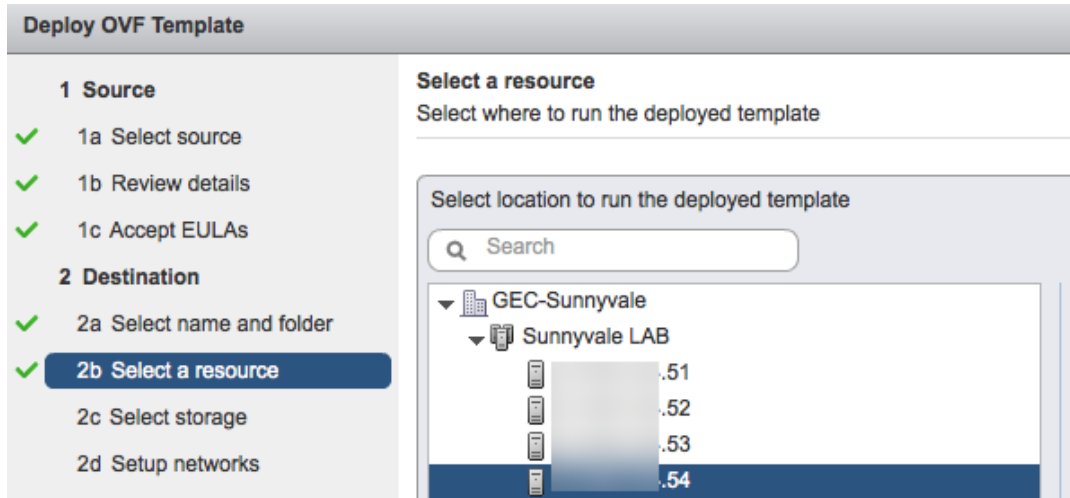
6. Select **Local File**, then click **Browse**.
7. Navigate to the folder where you extracted the files, then click **Next**.
The **Review Details** screen opens.
8. Review the information presented, then click **Next**.
The **Accept EULAs** screen opens.
9. Read the End User License Agreements (EULA)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

Figure 12 *Selecting the Name and Location for the Deployed Template*



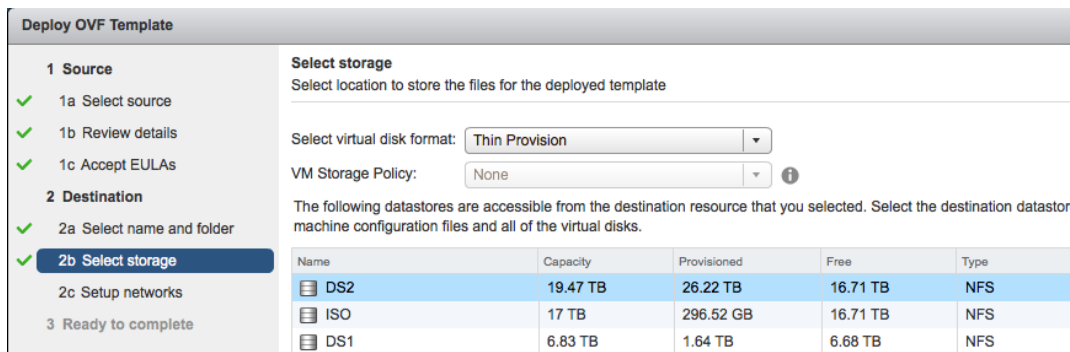
10. In the **Select Name and Folder** dialog:
 - The name of the template is set by default to *W-ClearPass Policy Manager Appliance*.
 - a. Change the name to the desired virtual appliance name.
 - b. Select the virtual appliance folder or data center where you want to deploy the W-ClearPass OVF file,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

Figure 13 *Selecting a Resource*



11. If required, choose the VMware host where W-ClearPass will be deployed, then click **Next**.
The **Select Storage** screen opens.

Figure 14 *Selecting the Location to Store the Files*



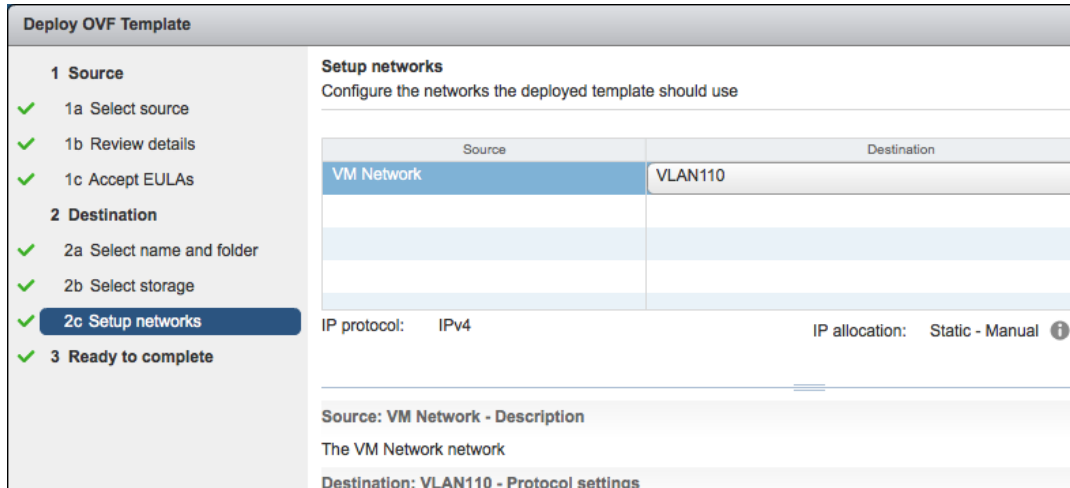
12. Choose the virtual disk format and data store for the W-ClearPass virtual appliance, then click **Next**.



The virtual disk format specified in [Figure 14](#) is **Thin Provision**. In a production environment, to ensure that the virtual appliance will not run out of disk space, Dell recommends using the **Thick Lazy Zeroed** virtual disk format.

The **Setup Networks** screen appears.

Figure 15 *Configuring the Networks for VM Deployment*



13. Specify the virtual network where W-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**.

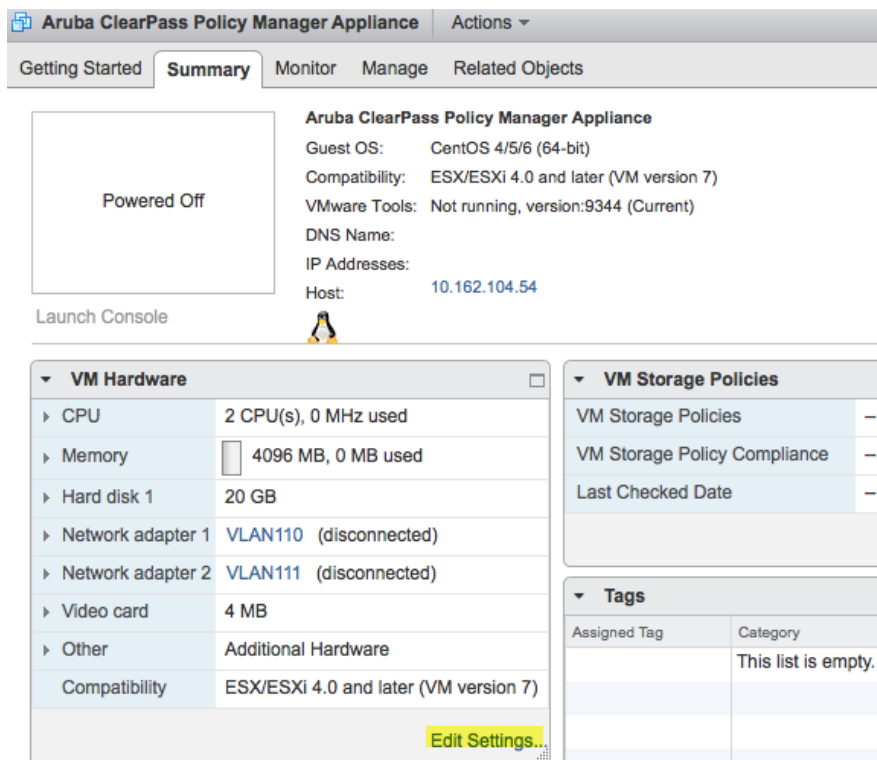
The OVF file is deployed in the selected network.

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 VM hardware and make sure that the network adapters are assigned correctly.

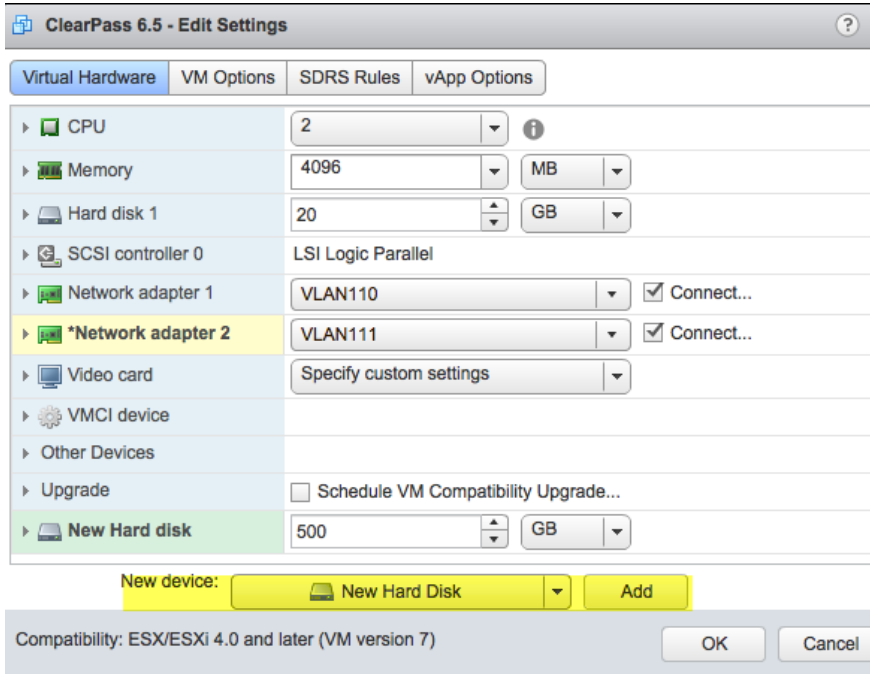
1. From the W-ClearPass Policy Manager Appliance, select the **Summary** tab.

Figure 16 *Virtual Appliance Summary Tab*



2. Click **Edit Settings**.
The **Edit Settings** dialog opens.

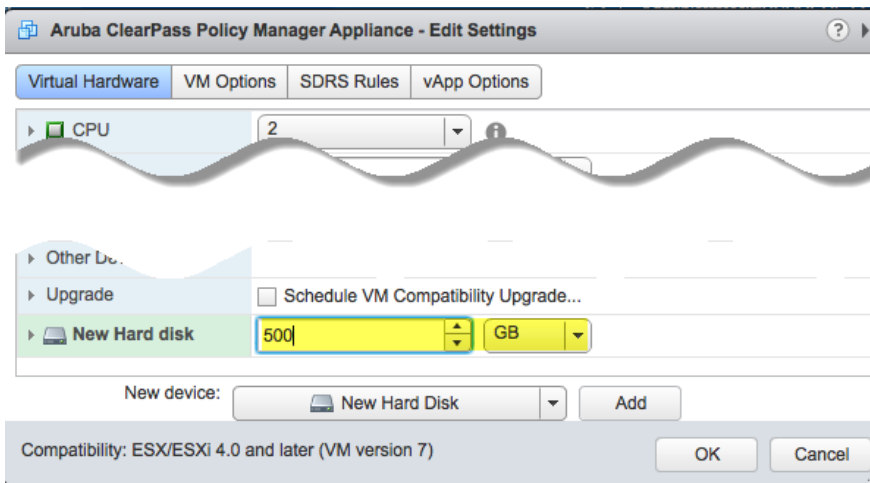
Figure 17 *Editing the Virtual Machine Settings*



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

The **Virtual Hardware** dialog opens.

Figure 18 *Specifying the Size of the New Hard Disk*



- d. Enter the size of the new hard disk, then click **OK**.



For the latest information on the recommended disk sizes for a virtual hard disk, refer to the W-ClearPass Release Notes at <https://download.dell-pcw.com> under the W-ClearPass 6.6 Upgrade folder. Access to this site requires log-in credentials.

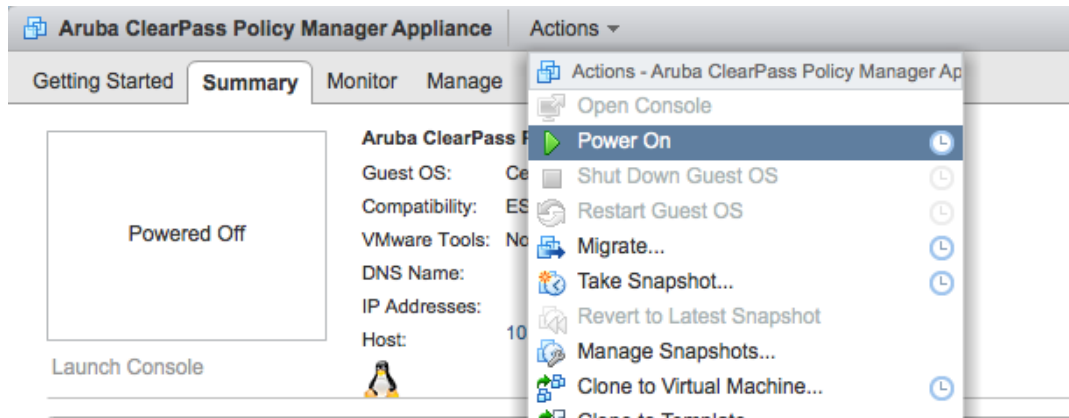
4. Make sure that the network adapters are assigned correctly:
 - a. **Network adapter 1: Management port**
 - b. **Network adapter 2: Data port**
 - c. Click **OK**.

Launching the W-ClearPass Virtual Appliance

To launch the W-ClearPass virtual appliance:

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

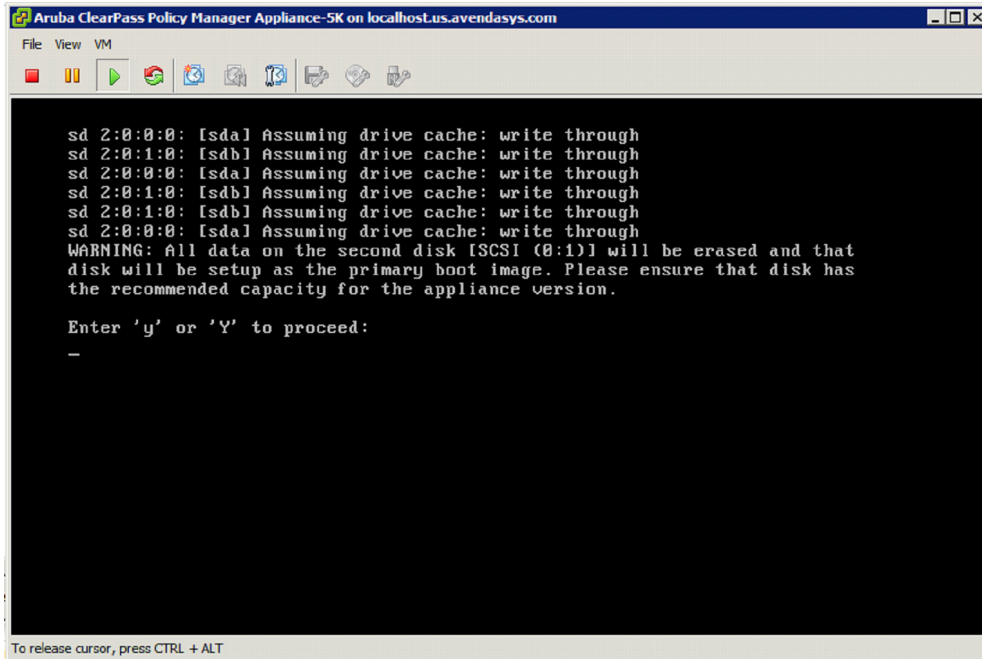
Figure 19 *Powering on the Virtual Machine*



The virtual appliance is now powered on.

2. To launch the VM console, choose **Actions** > **Launch Console**.
The initial VM console screen is displayed.

Figure 20 Initial Virtual Machine Console Screen



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

W-ClearPass setup and installation begins.

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

When the rebooting process is complete, the W-ClearPass virtual appliance is configured, and the virtual appliance will power on and boot up within a couple of minutes.



The whole process, from deploying the OVF image to the login banner screen, should take between 30 and 40 minutes.

4. After the W-ClearPass virtual appliance launches correctly, the virtual machine login banner is displayed.
5. 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 W-ClearPass server configuration information listed in [Table 6](#).
2. **Log in to the virtual appliance** using the following preconfigured credentials:
 - login: **appadmin**
 - password: **eTIPS123**

This initiates the Policy Manager Configuration wizard.

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

Follow the prompts, replacing the placeholder entries in the following illustration with the information you entered in [Table 6](#).

- 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 40](#).

- 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 W-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 6](#).
- #### 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 W-ClearPass license, which is described in the next section.

Applying and Activating the W-ClearPass License



Activating the W-ClearPass license is necessary for the virtual appliance only, not the hardware appliance, because the W-ClearPass license is included with the hardware appliance.

To activate and apply the W-ClearPass license:

1. After the configuration has been applied at the virtual appliance console, open a web browser and go to the management interface of W-ClearPass: **https://x.x.x.x/tips/**, where **x.x.x.x** is the IP address of the management interface defined for the W-ClearPass server in [Table 6](#).
2. Accept any security warnings from your browser regarding the self-signed SSL certificate, which comes installed in W-ClearPass by default.
The **Enter License Key** screen is displayed.

Figure 21 Entering the License Key

To continue, please enter the product license key

Select Application: Policy Manager

Enter license key: SP5D-UPJLXQ-375N-N562FO-CDFOD3-DG8D-ZNS7WK-JJPZUC-PR23-DCPTQA

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement (“Agreement”)

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY “ARUBA”). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED

I agree to the above terms and conditions.

Add License

3. Do the following:
 - a. In the **Select Application** drop-down, make sure the application is set to **Policy Manager**.
 - b. Make sure the **I agree to the above terms and conditions** check box is enabled.
 - c. In the **Enter license key** text box, enter your W-ClearPass license key.
 - d. Click **Add License**.

Upon successfully entering the license key, the **Admin Login** screen opens with a message indicating that you have 90 days to activate the product and a link to activate the product.

Figure 22 Activating W-ClearPass

You have 90 day(s) to activate the product

 [Activate Now](#)

Admin Login

Username:

Password:

Log In

4. To activate W-ClearPass on this virtual appliance, click **Activate Now**.

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

If the W-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 23](#).

Figure 23 *Performing Offline Activation*

The screenshot shows a web interface for product activation. At the top, a red banner reads "You have 90 day(s) to activate the product". Below this, there are three main sections: "Online Activation" with an "Activate Now" button; "Offline Activation" which includes instructions for downloading a token, emailing support at support@arubanetworks.com, and uploading an activation key; and "Update License" with an "Update License" button.

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

Logging in to the W-ClearPass Virtual Appliance

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

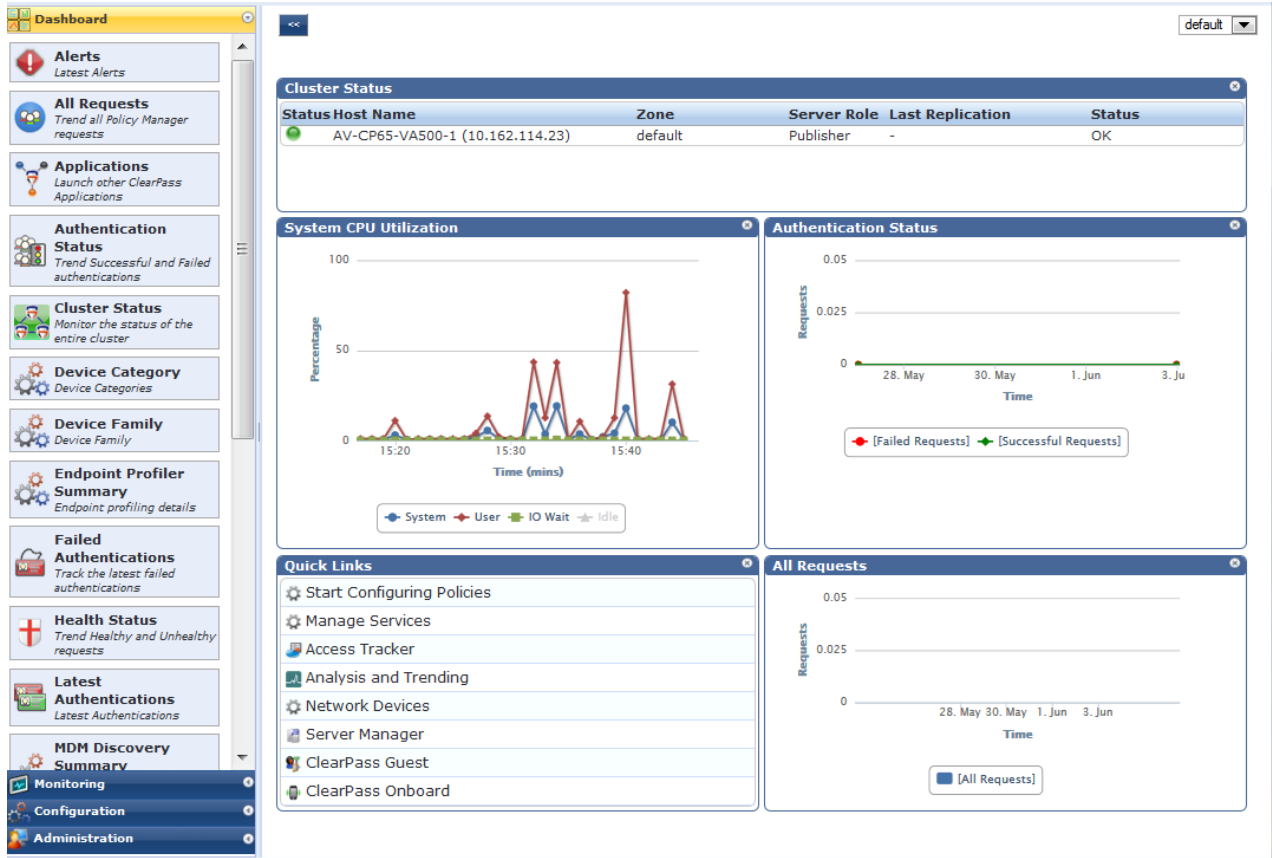
Figure 24 *Logging in to the W-ClearPass Virtual Appliance*

The screenshot shows the "Admin Login" dialog box. It has a title bar "Admin Login" and two input fields: "Username:" with the text "admin" and "Password:" with masked characters "*****". A "Log In" button is located at the bottom of the dialog.

1. Log in to the W-ClearPass virtual appliance with the following credentials:
 - **Username:** admin
 - **Password:** Enter the cluster password defined in [Completing the Virtual Appliance Setup on page 36](#).
2. Click **Log In**.

The W-ClearPass Policy Manager opens.

Figure 25 W-ClearPass Policy Manager Landing Page



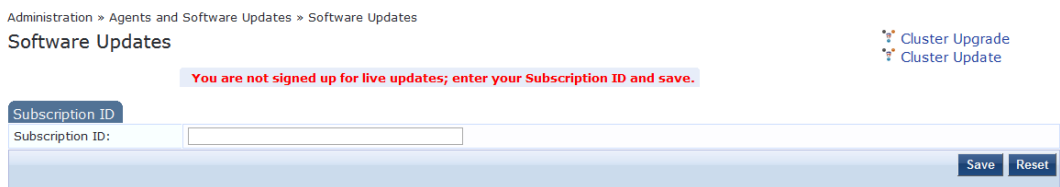
Signing Up for Live Software Updates

Upon your initial login to W-ClearPass Policy Manager, you need to register for software updates.

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

A message is displayed indicating that the W-ClearPass virtual appliance is not signed up for live updates and that you must enter your subscription ID.

Figure 26 Entering the Subscription ID for Live Updates



2. If the W-ClearPass Policy Manager server has Internet access, enter your subscription ID, then click **Save**.

After successfully applying the subscription ID, you will see a message indicating that the subscription ID was updated successfully and W-ClearPass is processing updates from the W-ClearPass Webservice.

Posture & Profile Data Updates are downloaded and installed automatically, while **Firmware & Patch Updates** are merely displayed.

Changing the Administration Password

When the cluster password for this W-ClearPass server is set upon initial configuration (see [Completing the Virtual Appliance Setup on page 36](#)), 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 W-ClearPass, navigate to **Administration > Users and Privileges > Admin Users**.

The **Admin Users** page opens.

Figure 27 Admin Users Page

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

Showing 1-2 of 2

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

The **Edit Admin User** dialog opens.

Figure 28 Changing the Administration Password

Edit Admin User

User ID: admin

Name: Super Admin

Password: ●●●●●●●●●●

Verify Password: ●●●●●●●●●●

Privilege Level: Super Administrator

Save Cancel

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

Powering Off the W-ClearPass Virtual Appliance

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

To power off the W-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 W-ClearPass virtual appliance shuts down.

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

This section documents the procedures for installing the W-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 W-ClearPass software updates and changing the admin password.

This section contains the following information:

- [Introduction](#)
- [Before Starting the W-ClearPass Installation](#)
- [W-ClearPass Hyper-V Virtual Appliance Installation Summary](#)
- [Importing the Virtual Machine](#)
- [Adding a Hard Disk to a Virtual Machine](#)
- [Launching the W-ClearPass Virtual Appliance](#)
- [Completing the Virtual Appliance Configuration](#)
- [Applying and Activating the W-ClearPass License](#)
- [Logging in to the W-ClearPass Virtual Appliance](#)
- [Signing Up for Live Software Updates](#)
- [Changing the Administration Password](#)
- [Powering Off the W-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

W-ClearPass Policy Managersupports the following Hyper-V hypervisors:

- Microsoft Windows Server 2012 R2 Enterprise with Hyper-V Role
- Microsoft Hyper-V Server 2012 R2



For the latest information on the supported hypervisors and virtual hardware requirements, refer to the appropriate version of the W-ClearPass Release Notes at <https://download.dell-pcw.com> under the W-ClearPass 6.6 Upgrade folder. Access to this site requires log-in credentials.

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 W-ClearPass Policy Manager 6.6 installations.

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

Supplemental Storage/Hard Disk Requirements

W-ClearPassHyper-V ships with a 20 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 48](#) for

details). The additional space required depends on the W-ClearPass virtual appliance version.

Processing and Memory Requirements

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

W-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. W-ClearPass Policy Manager requires a continuous sustained high data I/O rate.

Before Starting the W-ClearPass Installation

Before starting the installation and configuration procedures for the virtual appliance, determine the following information for the W-ClearPass server on your network, note the corresponding values for the parameters listed in [Table 7](#), and keep it for your records:

Table 7: W-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)	NOTE: 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)	

W-ClearPass Hyper-V Virtual Appliance Installation Summary

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

- 1.
1. Download the Microsoft Hyper-V package from the from the Dell Download site.
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.

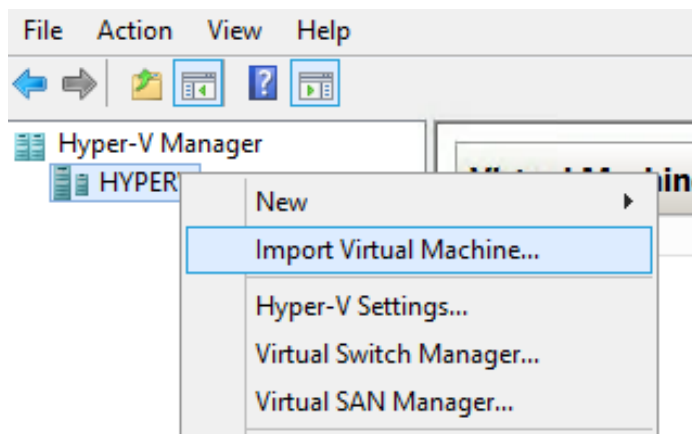
Importing the Virtual Machine

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.
1. Download the Microsoft Hyper-V package from the from the Dell Download site at <http://download.dell-pcw.com> to a folder accessible by your Microsoft Hyper-V server.
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 29 Selecting the "Import Virtual Machine" Option

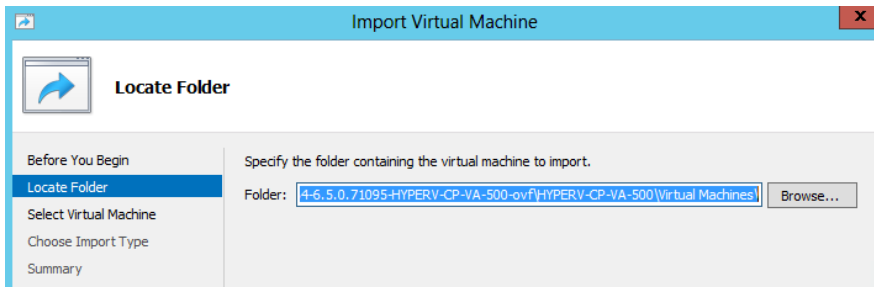


The **Before You Begin** dialog opens.

5. Click **Next**.

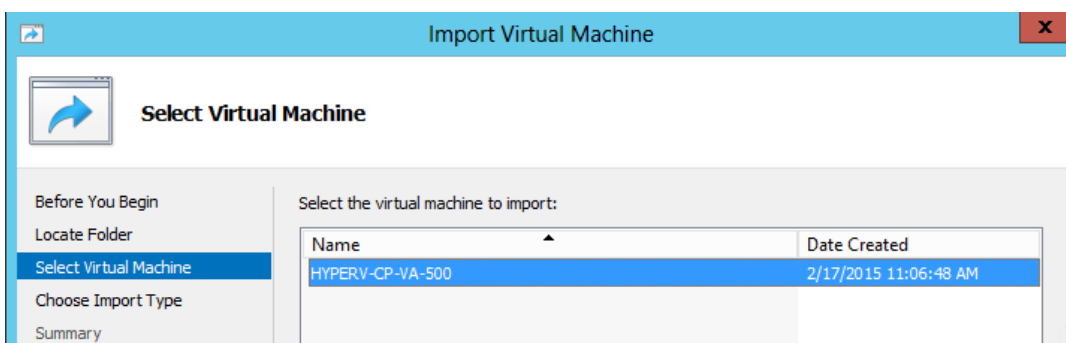
The **Locate Folder** dialog opens.

Figure 30 Locating the Folder



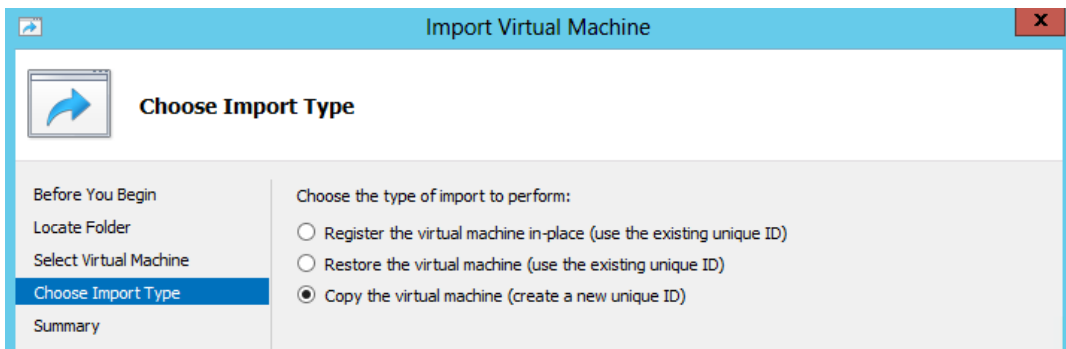
6. In the **Locate Folder** step, select the folder you unzipped in **Step 2**, then click **Next**.
The **Select Virtual Machine** dialog opens.

Figure 31 Selecting the Virtual Machine



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

Figure 32 Specifying the Import Type



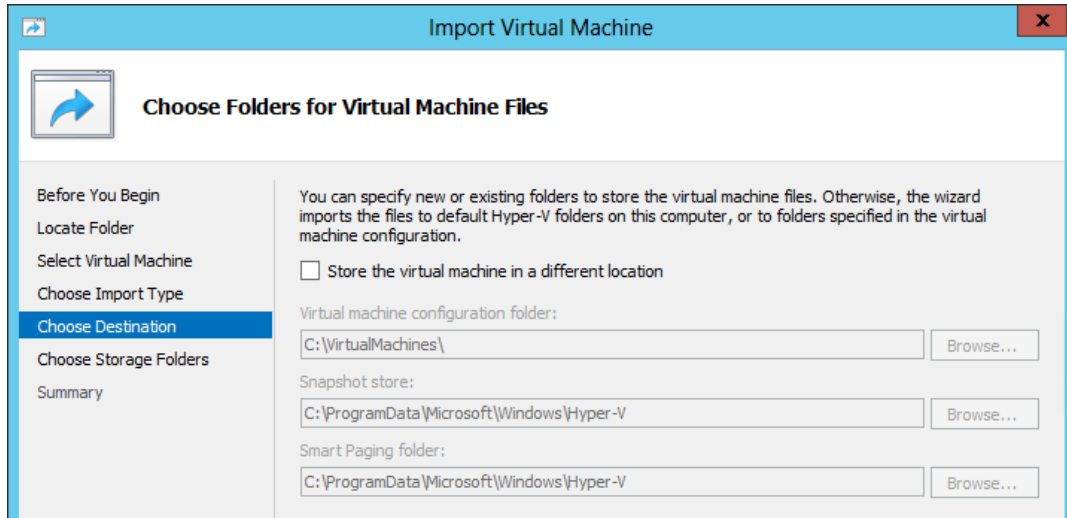
8. In the **Choose Import Type** step, select **Copy the virtual machine**, then click **Next**.



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.

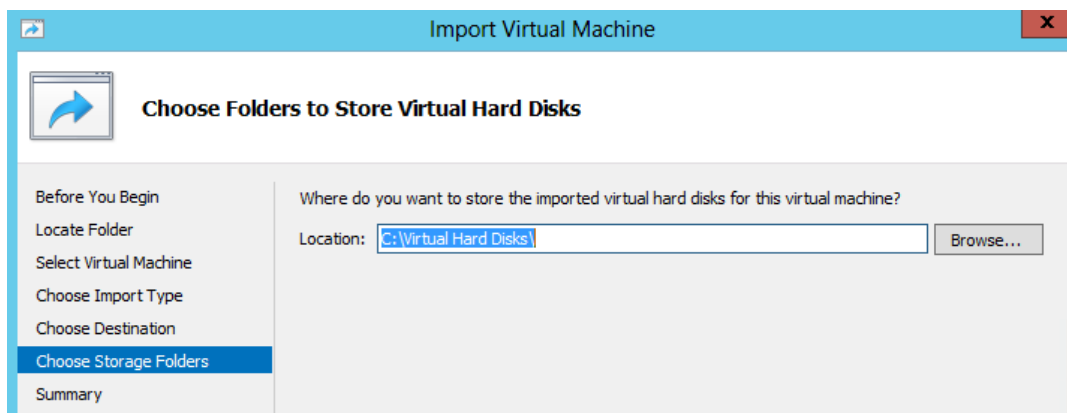
Figure 33 Specifying the Folders for the Virtual Machine Files



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 34 Specifying Folders to Store Virtual Hard Disks



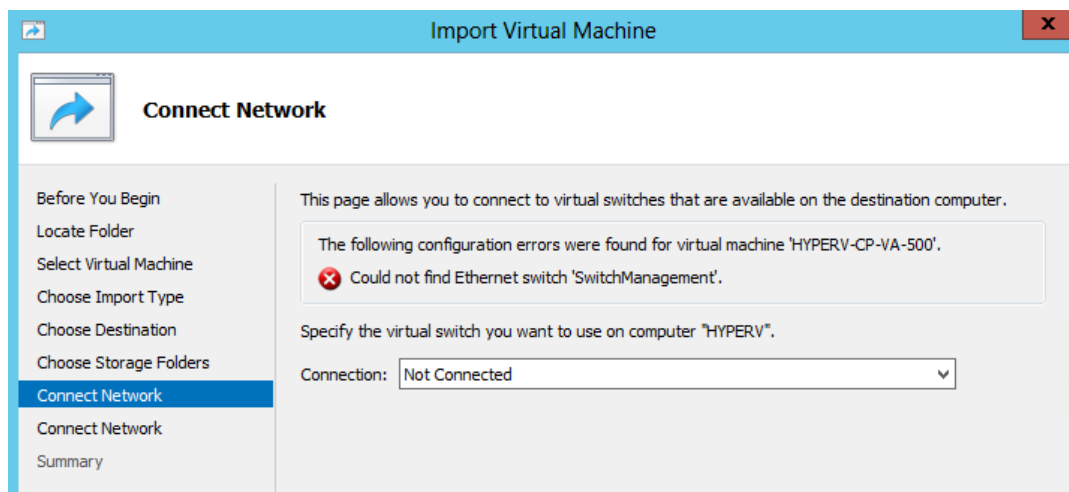
10. Accept the default virtual hard drive storage folder, or browse to a new location to change it to your preferred location, then click **Next**.



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.

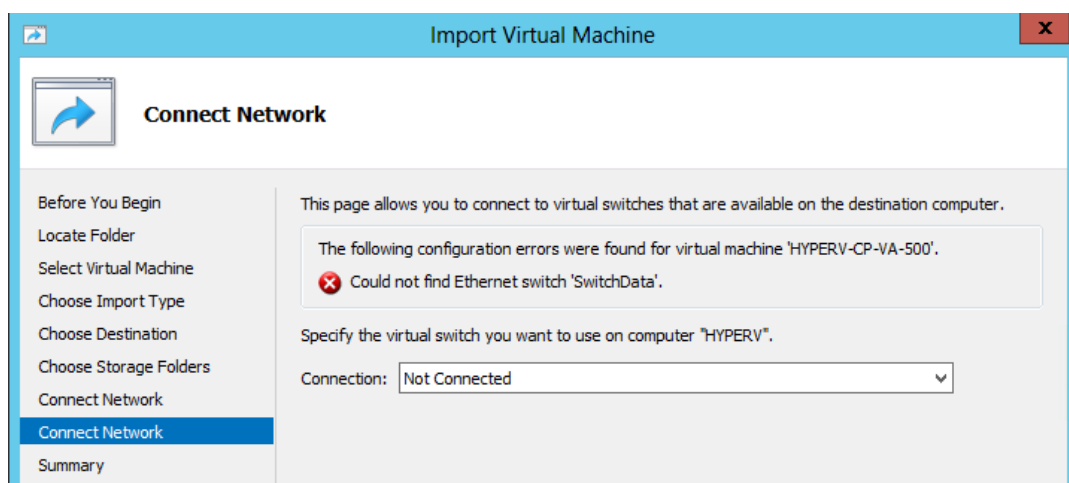
Figure 35 Specifying the Virtual Switch in the Event of an Error



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

Figure 36 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

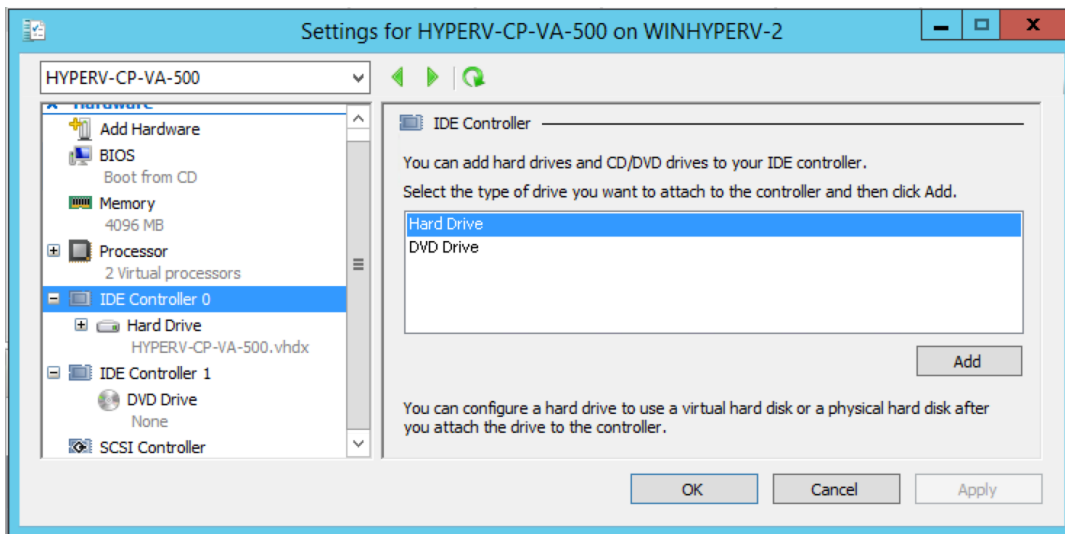


Do not create the virtual hard disk in a folder that is marked for encryption. Virtual hard disks are stored as .vhd files. Hyper-V does not support the use of storage media if Encrypting File System (EFS) has been used to encrypt the .vhd file. However, you can use files stored on a volume that uses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

To add a hard disk to a virtual machine:

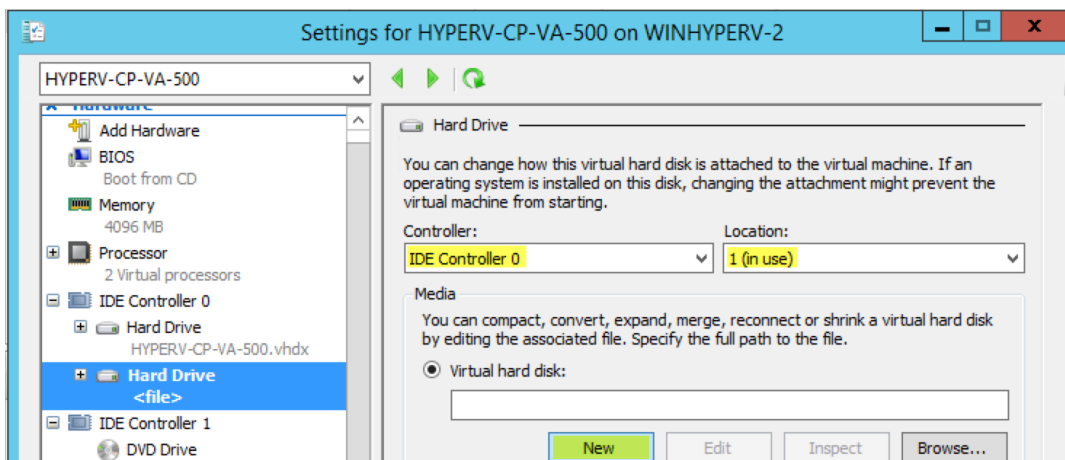
1. Open **Hyper-V Manager**.
2. In the **Results** pane, under **Virtual Machines**, select the virtual appliance that you want to configure.
3. In the **Action** pane, under the name of the virtual appliance, click **Settings**.
The **Settings** page opens.

Figure 37 Specifying the Controller



4. To select the controller to attach the virtual hard disk to, in the Navigation (left) pane, select **IDE Controller 0**, then click **Add**.
The **Hard Drive** dialog opens.

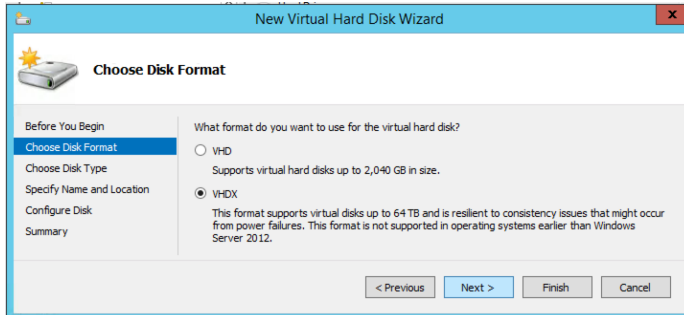
Figure 38 Configuring the Hard Drive



5. In the **Hard Drive** dialog:
 - a. **Controller:** Set to **IDE Controller 0**.
 - b. **Location:** Set to **1 (in use)**.

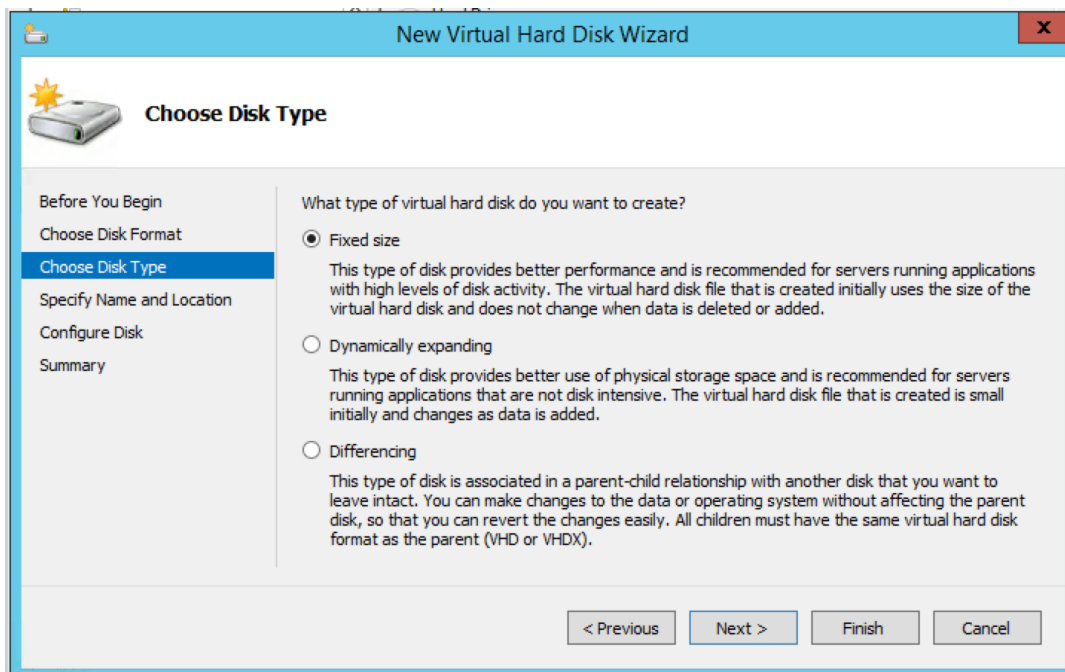
- Below the **Virtual hard disk** field, click **New**.
The **New Virtual Hard Disk Wizard** opens.
- From the **Before You Begin** dialog, click **Next**.
The **Choose Disk Format** dialog opens.

Figure 39 *Specifying the Disk Format*



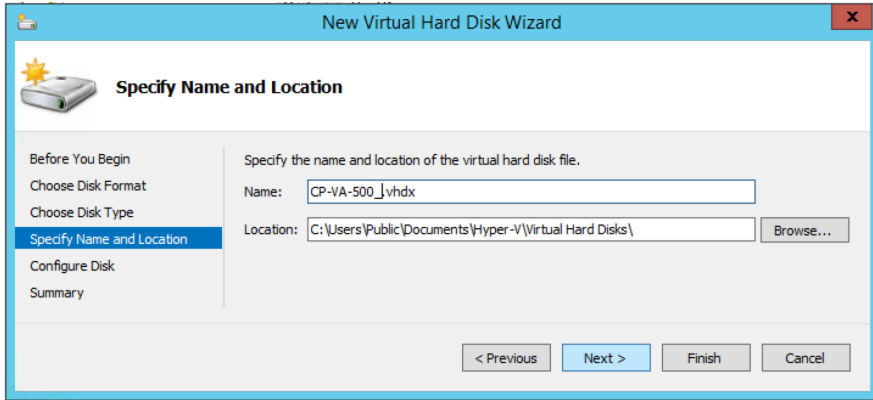
- For the disk format, choose **VHDX**, then click **Next**.
The **Choose Disk Type** dialog opens.

Figure 40 *Specifying the Virtual Hard Disk Type*



- For the disk type, choose **Fixed size**, then click **Next**.
The **Specify Name and Location** dialog opens.

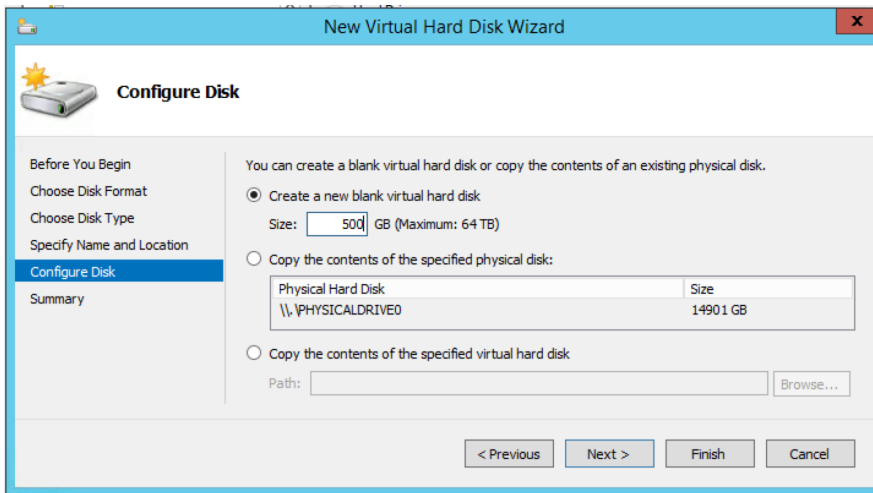
Figure 41 *Specifying the Name and Location of the Hard Disk File*



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 42 *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 W-ClearPass Release Notes at <https://download.dell-pcw.com> under the W-ClearPass 6.6 Upgrade folder. Access to this site requires log-in credentials.

- b. When finished, 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:

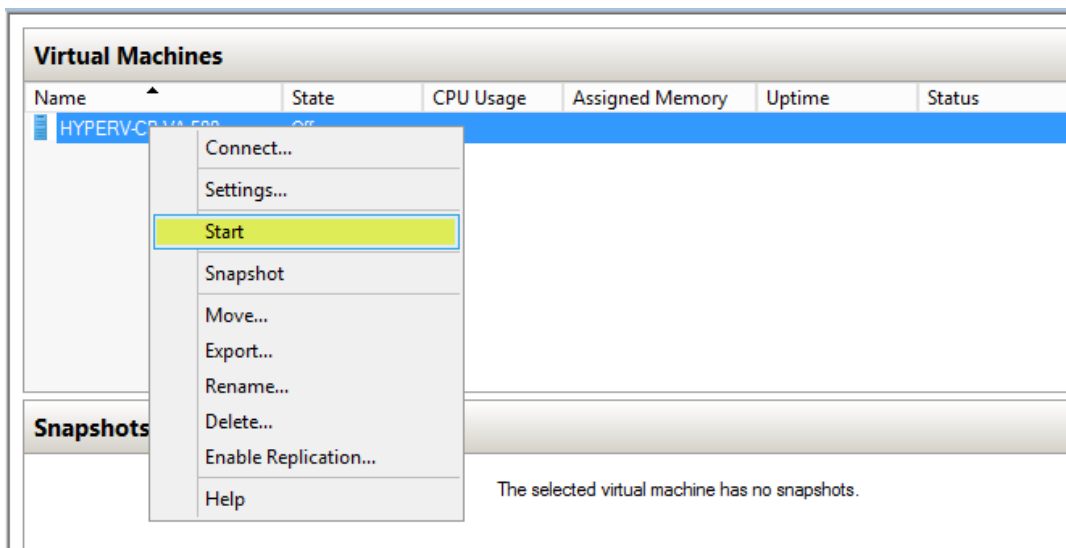
- By default, membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. However, an administrator can use Authorization Manager to modify the authorization policy so that a user or group of users can complete this procedure.
- Virtual hard disks are stored as .vhd 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 .vhd 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 W-ClearPass Virtual Appliance

To launch the W-ClearPass virtual appliance:

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

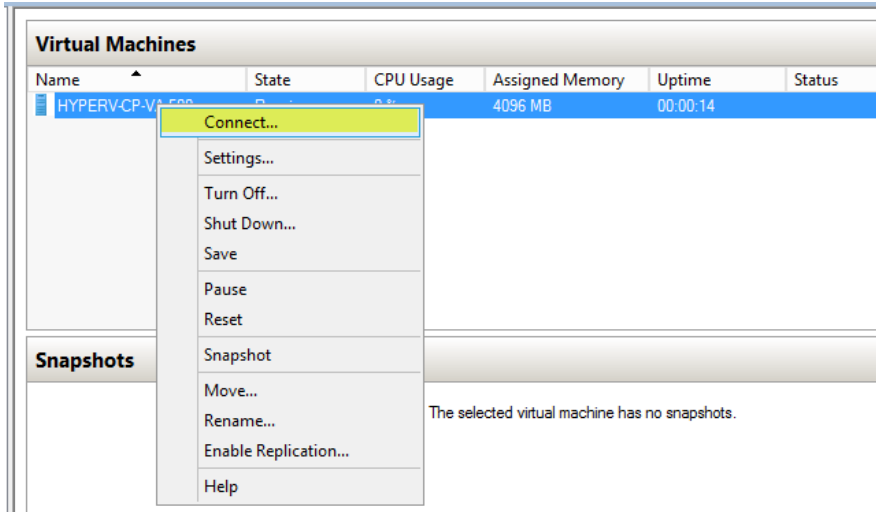
Figure 43 Starting the Virtual Machine



The virtual appliance powers on.

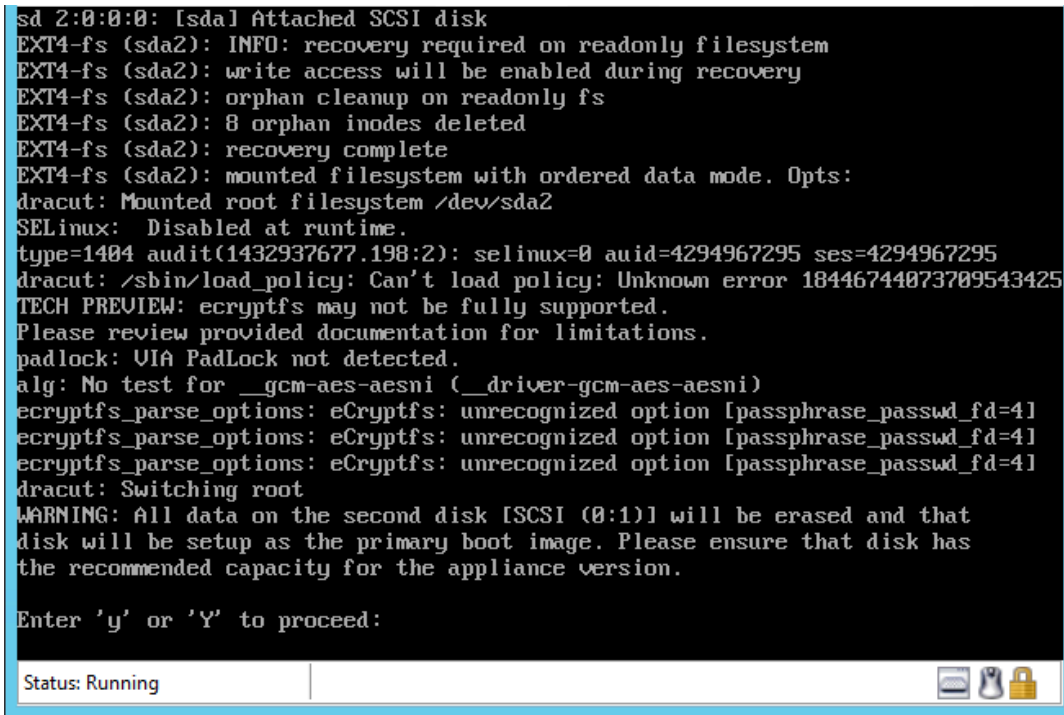
2. To launch the VM console, right-click the **name of the virtual machine**, then choose **Connect**.

Figure 44 *Launching the VM Console*



The initial virtual machine console screen is displayed.

Figure 45 *Initial Virtual Machine Console Screen*



- To proceed with the installation, enter **y**.
W-ClearPass setup and installation begins.
Two console screens appear sequentially—the first screen indicates that the W-ClearPass Installer is rebooting, and the second screen indicates that the virtual appliance is rebooting.
When the rebooting process is complete, the W-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.

4. After the W-ClearPass virtual appliance launches correctly, the virtual appliance login banner is displayed.
5. 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 W-ClearPass server configuration information listed in [Table 7](#).
2. **Log in to the virtual appliance** using the following preconfigured credentials :
 - login: **appadmin**
 - password: **eTIPS123**

This initiates the Policy Manager Configuration wizard.

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

Follow the prompts, replacing the placeholder entries in the following illustration with the information you entered in [Table 7](#).

- 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 56](#).

- 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 W-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 7](#).
 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 W-ClearPass license.

Applying and Activating the W-ClearPass License



Activating the W-ClearPass license is necessary for the virtual appliance only, not the hardware appliance, because the W-ClearPass license is included with the hardware appliance.

To activate and apply the W-ClearPass license:

1. After the configuration has been applied at the virtual appliance console, open a web browser and go to the management interface of W-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 W-ClearPass server in [Table 7](#).
2. Accept any security warnings from your browser regarding the self-signed SSL certificate, which comes installed in W-ClearPass by default.

The Enter License Key screen is displayed.

Figure 46 Entering the License Key

To continue, please enter the product license key

Select Application: Policy Manager

Enter license key: SP5D-UPILXQ-375N-N562FO-CDFOD3-DG8D-ZN57WK-JJP2UC-PR23-DCPTQA

Terms and Conditions

Aruba Networks, Inc. End-User Software License Agreement ("Agreement")

IMPORTANT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY "ARUBA"). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED

I agree to the above terms and conditions.

Add License

3. Do the following:
 - a. In the **Select Application** drop-down, make sure the application is set to **Policy Manager**.
 - b. Make sure the **I agree to the above terms and conditions** check box is enabled.
 - c. In the **Enter license key** text box, enter your W-ClearPass license key.
 - d. Click **Add License**.

Upon successfully entering the 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 47 Activating W-ClearPass

You have 90 day(s) to activate the product

Admin Login

Username:

Password:

Log In

4. To activate W-ClearPass on this virtual appliance, click **Activate Now**.

W-ClearPass Policy Manager attempts to activate the license over the Internet with W-Series license activation servers.

If the W-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 48](#).

Figure 48 *Performing Offline Activation*

The screenshot shows a web interface for product activation. At the top, a red banner reads "You have 90 day(s) to activate the product". Below this, there are three main sections: "Online Activation" with an "Activate Now" button; "Offline Activation" which includes instructions and three steps: 1. Download an Activation Request Token (with a "Download" button), 2. Email the Activation Request Token to Aruba Networks Support (support@arubanetworks.com), and 3. Upload the Activation Key received from Aruba Networks Support (with a file selection field and an "Upload" button); and "Update License" with an "Update License" button.

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

Logging in to the W-ClearPass Virtual Appliance

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

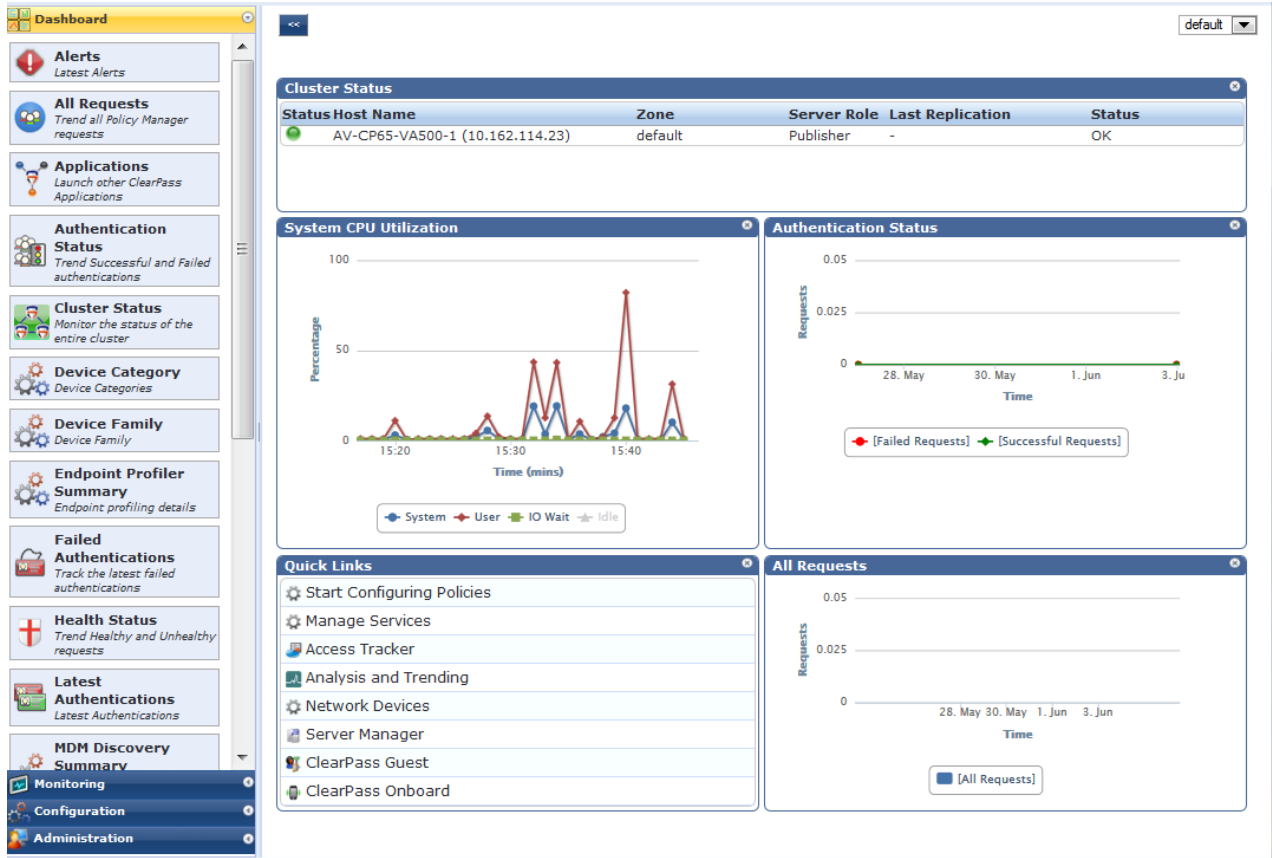
Figure 49 *Logging in to the W-ClearPass Virtual Appliance*

The screenshot shows the "Admin Login" dialog box. It has a title bar "Admin Login" and two input fields: "Username:" with the text "admin" and "Password:" with masked characters "*****". Below the fields is a "Log In" button.

1. Log in to the W-ClearPass virtual appliance with the following credentials:
 - **Username:** admin
 - **Password:** Enter the cluster password defined in [Completing the Virtual Appliance Configuration on page 53](#).
2. Click **Log In**.

The W-ClearPass Policy Manager Landing Page opens.

Figure 50 W-ClearPass Policy Manager Landing Page



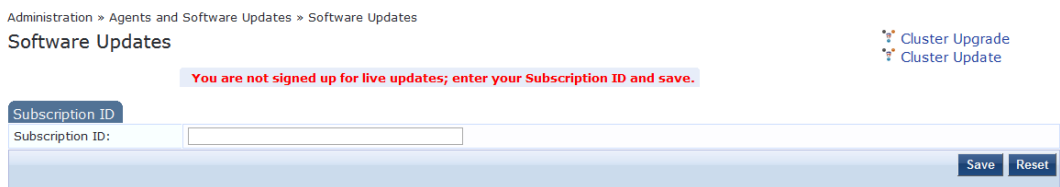
Signing Up for Live Software Updates

Upon your initial log-in to W-ClearPass Policy Manager, you should register for live software updates.

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

A message is displayed indicating that the W-ClearPass virtual appliance is not signed up for live updates and that you must enter your **subscription ID**.

Figure 51 Entering the Subscription ID for Live Updates



2. If the W-ClearPass Policy Manager server has Internet access, enter your **subscription ID**, then click **Save**.

After successfully applying the subscription ID, you will see a message indicating that the subscription ID was updated successfully and W-ClearPass is processing updates from the W-ClearPass Webservice.

Note that **Posture & Profile Data Updates** are downloaded and installed automatically, while Firmware & Patch Updates are merely displayed.

Changing the Administration Password

When the cluster password for this W-ClearPass server is set upon initial configuration (see [Completing the Virtual Appliance Configuration on page 53](#)), 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 W-ClearPass, navigate to **Administration > Users and Privileges > Admin Users**.
The **Admin Users** page opens.

Figure 52 Admin Users Page

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

2. Select the appropriate **admin** user.
The **Edit Admin User** dialog opens.

Figure 53 Changing the Administration Password

User ID:	admin
Name:	Super Admin
Password:
Verify Password:
Privilege Level	Super Administrator

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

Powering Off the W-ClearPass Virtual Appliance

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

To power off the W-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 W-ClearPass virtual appliance shuts down.

Accessing the W-ClearPass Administrative Interface

This section contains the following information:

- [Supported Browsers](#)
- [Accessing the Administrative Interface](#)
- [Changing the Administration Password](#)

- [Accessing W-ClearPass Online Help](#)

Supported Browsers

The supported browsers for W-ClearPass are:

- Mozilla Firefox on Windows Vista, Windows 7, Windows 8.x, Windows 10, and Macintosh OS X
- Google Chrome for Macintosh OS X and Windows
- Apple Safari 3.x and later on Macintosh OS X
- Mobile Safari 5.x on iOS
- Microsoft Internet Explorer 10 and later on Windows 7 and Windows 8.x



NOTE

When accessing W-ClearPass Insight with Internet Explorer (IE), IE 11 or above is required.

- Microsoft Edge on Windows 10

Accessing the Administrative Interface

To access the W-ClearPass Policy Manager administrative interface:



NOTE

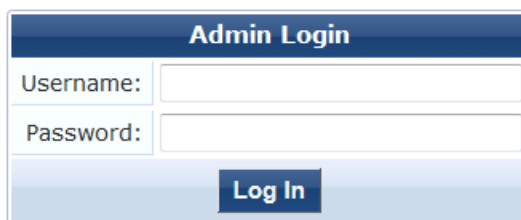
Use *Firefox (3.0 or higher)* or *Internet Explorer (7.0.5 or higher)*.

1. Navigate to *https://<hostname>/tips*, where *<hostname>* is the host name you configured during the initial configuration (for details, see [Configuring the W-ClearPass Hardware Appliance on page 22](#)).
 - If you're accessing W-ClearPass via a virtual machine, you are prompted to enter the license key. The following screen opens.

Figure 54 *Activating W-ClearPass*

You have 58 day(s) to activate the product

 [Activate Now](#)

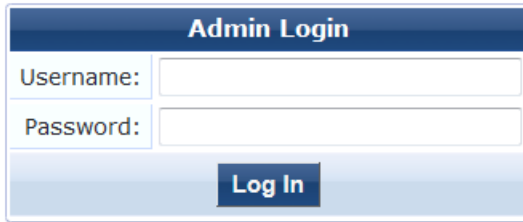


The image shows a screenshot of the 'Admin Login' form. It has a dark blue header with the text 'Admin Login'. Below the header, there are two input fields: 'Username:' and 'Password:'. At the bottom of the form is a blue button labeled 'Log In'.

2. If the W-ClearPass appliance is connected to the Internet, click **Activate Now**.
 - If the W-ClearPass appliance is *not* connected to the Internet, click **Download** to download the Activation Request Token.
3. Contact [Dell Support](#) and provide your technician with the downloaded Activation Request Token as an attachment.
 - a. Once you receive the activation key from Dell Support, save it to a known location on your computer.
 - b. To select the activation key, return to this screen and click **Browse**.
 - c. To upload the activation key, click **Upload**.

W-ClearPass Policy Manager is now activated. The **Admin Login** dialog opens.

Figure 55 Admin Login Dialog



The Admin Login dialog box features a dark blue header with the text "Admin Login". Below the header are two input fields: "Username:" and "Password:". A "Log In" button is positioned at the bottom center of the dialog.

4. Log in using the following credentials, then click **Log In**:

- Username: **admin**
- Password: **eTIPS123**

Changing the Administration Password

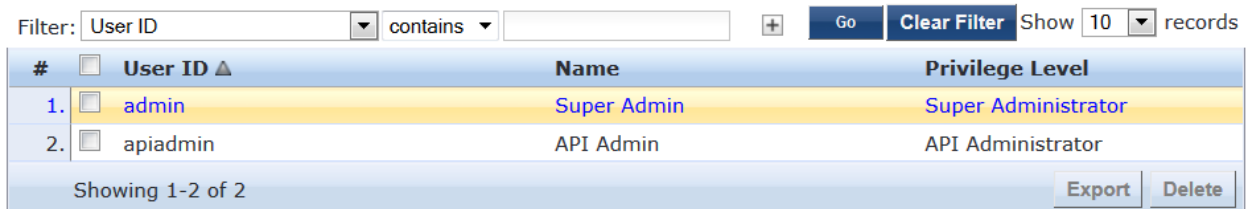
The recommended next task is to change the administration password for this W-ClearPass server.

To change the administration password:

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

The **Admin Users** page opens.

Figure 56 Admin Users Page



The Admin Users page includes a filter section at the top with a dropdown menu set to "User ID", a "contains" dropdown, and a search input field. To the right are "Go", "Clear Filter", and "Show 10 records" options. Below this is a table with three columns: "#", "User ID", "Name", and "Privilege Level".

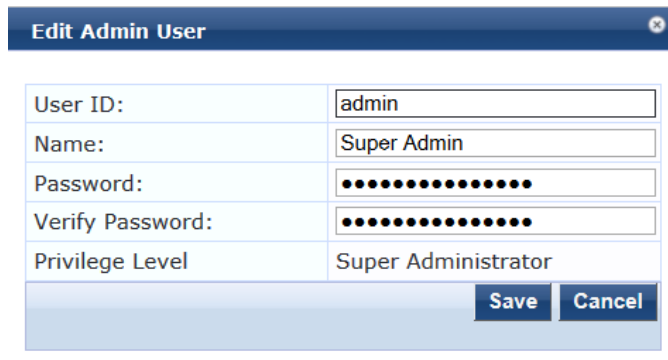
#	User ID	Name	Privilege Level
1.	admin	Super Admin	Super Administrator
2.	apiadmin	API Admin	API Administrator

At the bottom of the table, it says "Showing 1-2 of 2" and there are "Export" and "Delete" buttons.

2. Select the appropriate Admin user.

The **Edit Admin User** dialog appears.

Figure 57 Changing the Administration Password



The Edit Admin User dialog box has a dark blue header with the text "Edit Admin User". It contains several input fields: "User ID:" (with "admin" entered), "Name:" (with "Super Admin" entered), "Password:" (with masked characters), "Verify Password:" (with masked characters), and "Privilege Level" (with "Super Administrator" selected). "Save" and "Cancel" buttons are at the bottom right.

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

Accessing W-ClearPass Online Help

The *W-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 W-ClearPass screen.

Maintaining W-ClearPass Policy Manager Services

This section contains the following information:

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

Starting or Stopping W-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 W-ClearPass, navigate to **Administration > Server Manager > Server Configuration**.
The **Server Configuration** page opens.
2. Click the row that lists the W-ClearPass server of interest.
The **Server Configuration** screen for the selected W-ClearPass server opens.
3. Select the **Services Control** tab.
The **Services Control** page opens.

Figure 58 *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. DB change notification server	Running	Stop			
5. DB replication service	Running	Stop			
6. Micros Fidelio FIAS	Running	Stop			
7. Multi-master cache	Running	Stop			
8. Policy server	Running	Stop			
9. Radius server	Running	Stop			
10. System auxiliary services	Running	Stop			
11. System monitor service	Running	Stop			
12. Tacacs server	Running	Stop			
13. Virtual IP service	Stopped	Start			
14. AMG-AD Domain service	Running	Stop			

[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 this service is not being used.

- If a service is stopped, you can use its **Start** button to restart it.

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

Table 8: Description of the Server Configuration Page

Tab	Description	Comments
System	Displays server identity and connection parameters.	
Services Control	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.	
Service Parameters	This option allows you to change the system parameters for all services.	The options on this page vary based on the service selected.
System Monitoring	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.	This ensures that external Management Information Base (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.
Network	Use the Network page to: <ul style="list-style-type: none"> Create generic routing encapsulation (GRE) tunnels and VLANs related to guest users. Control which applications can have access to the node. 	<ul style="list-style-type: none"> A GRE tunnel creates a virtual point-to-point link between controllers over a standard IP network or the Internet. To create VLANs, your network infrastructure must support tagged 802.1Q packets on the physical interface selected. <p>NOTE: VLAN ID 1 is often reserved for use by certain network management components—avoid using this ID unless you know it will not conflict with a VLAN already defined in your network.</p>
FIPS	Enables W-ClearPass to operate in Federal Information Processing Standard mode.	For most users, this tab should be ignored. NOTE: Enabling FIPS mode resets the database.

Subset of CLI for W-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 W-ClearPass appliance hardware, or remotely using SSH, or use the VMware or Hyper-V console to run the virtual appliance.

```
*****
* Dell W-ClearPass Policy Manager                                     *
* Software Version : 6.6.0.62080                                     *
*****
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>
```

Flag/Parameter	Description
ip <mgmt data> <ip address>	<ul style="list-style-type: none">• Network interface type: <i>mgmt</i> or <i>data</i>• Server IP address
netmask <netmask address>	Netmask address
gateway <gateway address>	Gateway 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 W-ClearPass Policy Manager Appliance to the Active Directory Domain

If you are using Active Directory to authenticate users, be sure to join the W-ClearPass Policy Manager appliance to the Active Directory domain (for more information, see [Joining an Active Directory Domain on page 95](#)).

```
[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. NOTE: Use the Fully Qualified Domain Name.
[domain NetBIOS name]	Optional.

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

This chapter includes the following information:

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

Adding a Mobility Controller to W-ClearPass Policy Manager

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

To define a new mobility controller in W-ClearPass:

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

Figure 59 Network Devices Screen

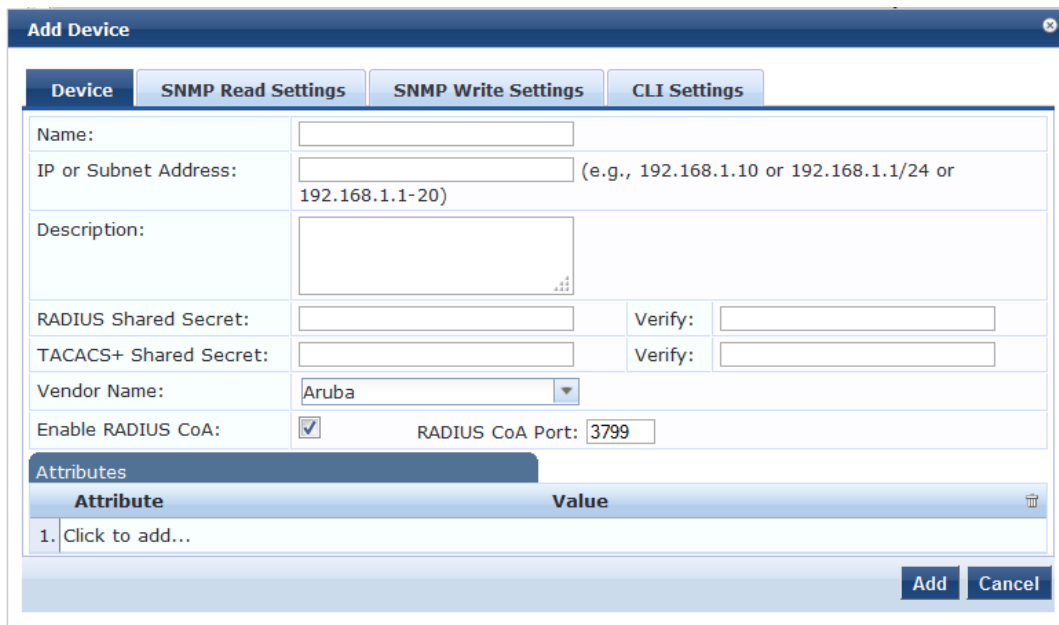


2. Click **Add**.

The **Add Device** wizard appears:

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

Figure 60 Add Device Wizard: Device Tab



3. Populate the **Network Device** parameters as described in [Table 9](#):

Table 9: Defining a Mobility Controller

Parameter	Action/Description
Name	1. Enter the name of the Mobility Controller.
IP or Subnet Address	2. Enter the IP address or subnet address of the Mobility Controller.

Parameter	Action/Description
Description	Dell recommends including a description of the device.
RADIUS Shared Secret	3. Specify the RADIUS Shared Secret for the current W-ClearPass Policy Manager server. NOTE: Make sure that the value of the Key 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 Table 10).
TACACS Shared Secret	If you're adding a device because you want W-ClearPass to manage access to that device with TACACS+, specify the TACACS+ Shared Secret.
Enable RADIUS CoA	4. 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.
RADIUS CoA Port	If RADIUS CoA is enabled, this specifies the default port 3799 . Change this value only if you defined a custom port on the mobility controller. For related information, see Configuring W-ClearPass as an RFC 3576 (CoA) Server .

5. 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 W-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 W-ClearPass.

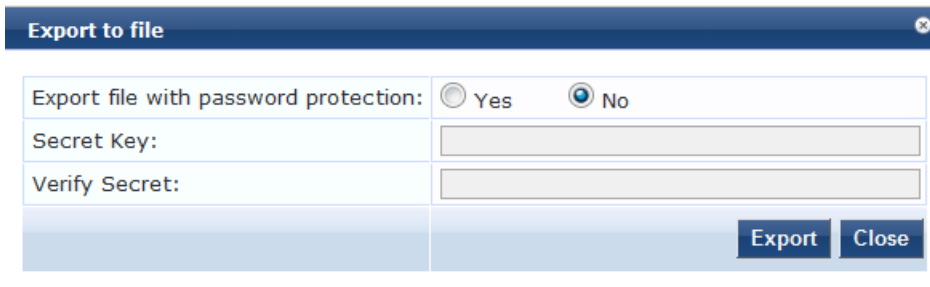
Generating an Example of Import File XML Format

To generate an example of the import file XML format:

1. From the **Network Devices** dialog, click **Add**.
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 61 *Export to File Dialog*



4. In the Export to file dialog, select **No** to the *Export file with password protection* field, then click **Export**.
5. Download the XML file.
6. Open the XML file in a text editor to view the format (see).

Figure 62 *Example of the Import File XML Format*

```
<?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <TipsContents xmlns="http://www.avendasys.com/tipsapiDefs/1.0">
  <TipsHeader version="6.5" exportTime="Thu Sep 03 03:17:55 IST 2015"/>
  - <NadClients>
    <NadClient ipAddress="192.168.1.1" radiusSecret="" tacacsSecret="" vendorName="Aruba"
      coaCapable="true" coaPort="3799" name="testdevice" description=""/>
  </NadClients>
</TipsContents>
```

Adding a W-ClearPass/RADIUS Server to the Mobility Controller

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

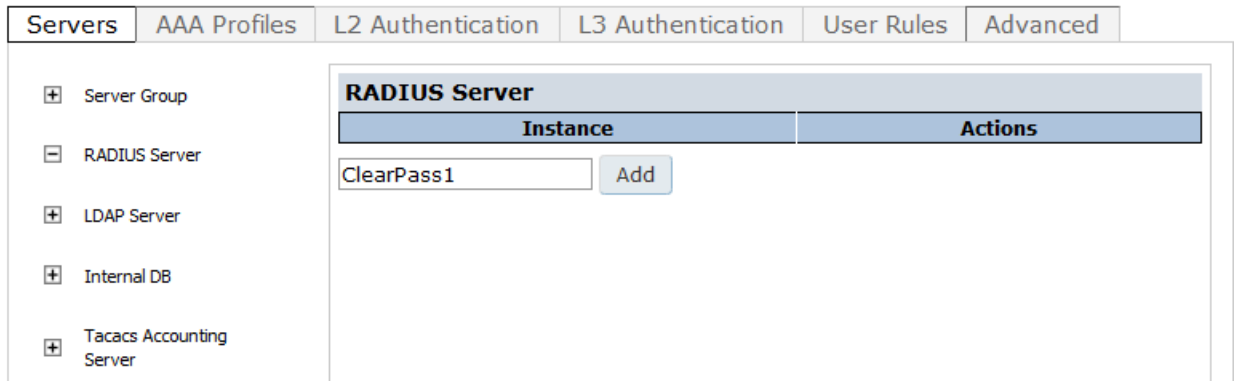
By adding the W-ClearPass/RADIUS server to the mobility controller, you are configuring the mobility controller to send authentication requests to the W-ClearPass/RADIUS server.

To define the W-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 63 Defining the RADIUS Server in the Mobility Controller

Security > Authentication > Servers



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

- Click the name of the new RADIUS server.

The **RADIUS Server** configuration screen opens.

Figure 64 Configuring the RADIUS Server

Host	10.100.0.1
Key	<input type="password"/> Retype: <input type="password"/>
CPPM credentials	cppm_username <input type="text" value="testTech"/> <input type="password"/> cppm_password Retype: <input type="password"/> <input type="password"/>
Auth Port	1812
Acct Port	1813
Radsec Port	2083
Retransmits	3
Timeout	5 sec
NAS ID	<input type="text"/>
NAS IP	<input type="text"/>
Enable IPv6	<input type="checkbox"/>
NAS IPv6	<input type="text"/>
Source Interface	vlanid <input type="text"/> ipv6addr <input type="text"/>
Use MD5	<input type="checkbox"/>
Use IP address for calling station ID	<input type="checkbox"/>
Mode	<input checked="" type="checkbox"/>
Lowercase MAC addresses	<input type="checkbox"/>
MAC address delimiter	none ▼
Service-type of FRAMED-USER	<input type="checkbox"/>
Radsec	<input type="checkbox"/>
Radsec Trusted CA Name	<input type="text"/>
Radsec Server Cert Name	<input type="text"/>
Radsec Client Cert	<input type="text"/>

7. Specify the values for the RADIUS server configuration parameters as described in [Table 10](#).

Table 10: *Configuring RADIUS Server Parameters on the Mobility Controller*

RADIUS Server Parameter	Action/Description	Comments
Host	<p>1. Specify the IP address or the fully qualified domain name of the RADIUS server.</p> <p>NOTE: In this case, specify the IP address of the W-ClearPass server, which is a RADIUS server.</p>	When you first add the RADIUS server, the mobility controller populates the Host field with a dummy IP address—127.0.0.1.
Key	<p>2. Enter the RADIUS shared secret that is configured on the authentication server (in this case, the W-ClearPass server).</p> <p>NOTE: The RADIUS Key value on the controller and the RADIUS Shared Secret on the W-ClearPass server must be identical.</p>	The maximum length is 128 characters.
CPPM credentials	<p>3. Enter the W-ClearPass server credentials if you want the mobility controller to use a configurable username and password instead of a support password.</p>	
Auth Port	<p>4. Specify the authentication port on the RADIUS server.</p>	<ul style="list-style-type: none"> • Range: 1 to 65535 • Default: 1812
Acct Port	<p>5. Specify the accounting port on the RADIUS server.</p>	<ul style="list-style-type: none"> • Range: 1 to 65535 • Default: 1813
Radsec Port	<p>6. Specify the Radsec (Secure RADIUS Service) port number of this server.</p>	<ul style="list-style-type: none"> • Range: 1 to 65535 • Default: 2083
Retransmits <number>	<p>7. Enter the maximum number of retries sent to the server by the mobility controller before the server is marked as down.</p>	<ul style="list-style-type: none"> • Range: 0 to 3 • Default: 3
Timeout <seconds>	<p>8. Enter the maximum time, in seconds, that the mobility controller waits before timing out the request and resending it.</p>	<ul style="list-style-type: none"> • Range: 0 to 30 • Default: 5
NAS ID	<p>Optional: Enter the Network Access Server (NAS) identifier to use in RADIUS packets. The NAS in this case is the Mobility Controller.</p>	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.

RADIUS Server Parameter	Action/Description	Comments
NAS IP	<p>9. Specify the NAS IP address to send in RADIUS packets.</p> <ul style="list-style-type: none"> To set the global NAS IP address, enter the following command: <pre>ip radius nas-ip <ip_addr></pre> 	<p>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.</p>
Enable IPv6	<p>To enable the operation of the RADIUS server over IPv6, check the Enable IPv6 check box.</p>	<p>Enabling IPv6 also enables the RADIUS attributes used to support IPv6 network access.</p>
Source Interface	<p>10. Enter a VLAN number ID. This allows you to use source IP addresses to differentiate RADIUS requests.</p> <ul style="list-style-type: none"> VLAN ID: Specify vlanid for the source interface when the RADIUS packets are sent to the RADIUS server via IPv4. IPv6 address: Specify ivpv6addr for the source interface when the RADIUS packets are sent to the RADIUS/W-ClearPass Policy Manager server via IPv6. <p>NOTE: 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"> 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. 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 is used.
Use MD5	<p>11. Enable this option to use an MD5 hash instead of a clear text password.</p>	<p>This option is disabled by default.</p>
Use IP address for calling station ID	<p>12. Enable this option if you choose to use an IP address instead of a MAC address for calling station IDs.</p>	<p>This option is disabled by default.</p>
Mode	<p>13. Enable this option if you want to enable the RADIUS server.</p>	<p>The Mode parameter defines whether the controller should or should not send RADIUS requests to the RADIUS/W-ClearPass server. This option is enabled by default.</p>
Lowercase MAC address	<p>Sends the MAC address in lowercase in the authentication and accounting requests to this server.</p>	<p>Default: Disabled</p>

RADIUS Server Parameter	Action/Description	Comments
MAC address delimiter	<p>14. Optionally, specify a MAC address delimiter. Sends the MAC address with the following delimiters in the authentication and accounting requests of this server:</p> <ul style="list-style-type: none"> ● colon: Send MAC address as: XX:XX:XX:XX:XX:XX ● dash: Send MAC address as: XX-XX-XX-XX-XX-XX ● none: Send MAC address as: XXXXXXXXXXXX ● oui-nic: Send MAC address as: XXXXXX-XXXXXX 	Default: None
Service-type of FRAMED-USER	15. Enable this option to send the service-type as FRAMED-USER instead of LOGIN-USER .	Default: Disabled
Radsec	16. Enable or disable RADIUS over TLS (Secure RADIUS Service) for this server.	Default: Disabled
Radsec Trusted CA Name	17. Enter the trusted Certificate Authority (CA) name to be used to verify this server.	
Radsec Server Cert Name	18. Enter the name of the trusted Radsec server certificate.	
Radsec Client Cert	19. Enter the name of the Radsec client certificate that the mobility controller should use for Radsec requests.	
called-station-id	<p>20. Specify the MAC address of the mobility controller. This parameter allows you to send different values for Called Station ID. Configure the following parameters for Called Station ID:</p> <ul style="list-style-type: none"> ● csid_type: Called station ID type. Default: macaddr ● include_ssid: Enabling this option includes the SSID in the Called Station ID along with csid_type. Default: Disabled ● csid_delimiter: Enabling this option allows you to send this delimiter to separate csid_type and ssid in the Called Station ID. Default: colon (Example: 00-1a-1e-00-1a-b8:dotx-ssid) 	
	21. When finished, click Apply .	The message "Configuration Updated successfully" is displayed.

Adding the W-ClearPass/RADIUS Server to a Server Group

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

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

Figure 65 Server Group Page

The screenshot shows the configuration page for Server Groups. At the top, there are tabs for Configuration, Diagnostics, and Maintenance, along with a Save Configuration button. The main navigation pane shows Security > Authentication > Servers. Under Servers, there are sub-tabs for AAA Profiles, L2 Authentication, L3 Authentication, User Rules, and Advanced. The left sidebar lists Server Group, RADIUS Server, and LDAP Server. The main content area displays a table for Server Groups with columns for Instance, Servers out of Service, and Actions. The table lists 'default' and 'internal' server groups. Below the table, there is an input field containing 'ClearPassGroup1' and an 'Add' button.

Instance	Servers out of Service	Actions
default		Show Reference Delete
internal		Show Reference Delete

ClearPassGroup1 Add

- 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.
- To configure the server group, click the **name of the new server group**.
The configuration screen for the selected server group opens.

Figure 66 Server Group Configuration Screen

Server Group > ClearPassGroup1 Show Reference Save As Reset

Fail Through

Load Balance

Servers

Name	Server-Type	trim-FQDN	Match-Rule
New	▲ ▼	Delete	

Server Rules

Priority	Attribute	Operation	Operand	Type	Action	Value	Validated
New	▲ ▼	Delete					

- To add a W-ClearPass Policy Manager server to the server group, in the **Servers** section, click **New**. The **Servers** configuration screen opens.
- To choose the W-ClearPass server for inclusion in the RADIUS server group, select the W-ClearPass (RADIUS) server name from the drop-down list (see [Figure 67](#)).

Figure 67 Selecting the W-ClearPass Server for Inclusion in the RADIUS Server Group

Server Group > ClearPassGroup1 Show Reference Save As Reset

Fail Through

Load Balance

Servers

Name	Server-Type	trim-FQDN	Match-Rule
Server Name	Trim FQDN	Match Type	Operator
Internal (Local) ▼	<input type="checkbox"/>	Authstring ▼	contains ▼
Internal (Local)		Add Rule	Delete Rule
ClearPass1 (Radius)			

Match String

Add Server Cancel

Server Rules

Priority	Attribute	Operation	Operand	Type	Action	Value	Validated
New	▲ ▼	Delete					

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

- If necessary, modify the **Servers** settings as needed, then click **Add Server**. You return to the **Server Group** configuration screen. The W-ClearPass Policy Manager server is now included in the RADIUS server group.

Figure 68 W-ClearPass Server Added to the RADIUS Server Group

The screenshot shows the configuration page for a server group named 'ClearPassGroup1'. At the top right, there are buttons for 'Show Reference', 'Save As', and 'Reset'. Below these are two checkboxes: 'Fail Through' and 'Load Balance', both of which are currently unchecked. The main section is titled 'Servers' and contains a table with the following data:

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

Below the table are buttons for 'New', up/down arrows, and 'Delete'. Underneath is a section for 'Server Rules' with a table that has the following headers: Priority, Attribute, Operation, Operand, Type, Action, Value, and Validated. Below this table are buttons for 'New', up/down arrows, and 'Delete'.

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

You have now defined the W-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 W-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 69 AAA Profiles Summary

AAA Profiles Summary								Actions
Name	Role	MAC Auth.	802.1x Auth.	RADIUS Acct.	XML-API Auth.	RFC 3576 Auth.		
bssidreorder	logon		default-psk				Show Reference Delete	
default	logon						Show Reference Delete	
default-dot1x	logon		default				Show Reference Delete	
default-dot1x-psk	logon		default-psk				Show Reference Delete	

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 70 AAA Profile Configuration Page

Configuration | Diagnostics | Maintenance | Save Configuration

Security > Authentication > Profiles

Servers	AAA Profiles	L2 Authentication	L3 Authentication	User Rules	Advanced																																
AAA	<ul style="list-style-type: none"> ClearPassAAAProfile MAC Authentication MAC Authentication Server Group default 802.1X Authentication 802.1X Authentication Server Group RADIUS Accounting Server Group XML API server RFC 3576 server david davidtest-aaa_prof default default-dot1x default-dot1x-psk default-mac-auth 	AAA Profile > ClearPassAAAProfile Show Reference Save As Reset																																			
		<table border="1"> <tr><td>Initial role</td><td>logon</td></tr> <tr><td>MAC Authentication Default Role</td><td>guest</td></tr> <tr><td>802.1X Authentication Default Role</td><td>guest</td></tr> <tr><td>Download Role from CPPM</td><td><input type="checkbox"/></td></tr> <tr><td>L2 Authentication Fail Through</td><td><input type="checkbox"/></td></tr> <tr><td>Multiple Server Accounting</td><td><input type="checkbox"/></td></tr> <tr><td>User idle timeout</td><td><input type="checkbox"/> Enable seconds <input type="text"/></td></tr> <tr><td>Max IPv4 for wireless user</td><td><input type="text" value="2"/></td></tr> <tr><td>RADIUS Interim Accounting</td><td><input type="checkbox"/></td></tr> <tr><td>User derivation rules</td><td>--NONE--</td></tr> <tr><td>Wired to Wireless Roaming</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>SIP authentication role</td><td>--NONE--</td></tr> <tr><td>Device Type Classification</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Enforce DHCP</td><td><input type="checkbox"/></td></tr> <tr><td>PAN Firewall Integration</td><td><input type="checkbox"/></td></tr> <tr><td>Open SSID radius accounting</td><td><input type="checkbox"/></td></tr> </table>				Initial role	logon	MAC Authentication Default Role	guest	802.1X Authentication Default Role	guest	Download Role from CPPM	<input type="checkbox"/>	L2 Authentication Fail Through	<input type="checkbox"/>	Multiple Server Accounting	<input type="checkbox"/>	User idle timeout	<input type="checkbox"/> Enable seconds <input type="text"/>	Max IPv4 for wireless user	<input type="text" value="2"/>	RADIUS Interim Accounting	<input type="checkbox"/>	User derivation rules	--NONE--	Wired to Wireless Roaming	<input checked="" type="checkbox"/>	SIP authentication role	--NONE--	Device Type Classification	<input checked="" type="checkbox"/>	Enforce DHCP	<input type="checkbox"/>	PAN Firewall Integration	<input type="checkbox"/>	Open SSID radius accounting	<input type="checkbox"/>
Initial role	logon																																				
MAC Authentication Default Role	guest																																				
802.1X Authentication Default Role	guest																																				
Download Role from CPPM	<input type="checkbox"/>																																				
L2 Authentication Fail Through	<input type="checkbox"/>																																				
Multiple Server Accounting	<input type="checkbox"/>																																				
User idle timeout	<input type="checkbox"/> Enable seconds <input type="text"/>																																				
Max IPv4 for wireless user	<input type="text" value="2"/>																																				
RADIUS Interim Accounting	<input type="checkbox"/>																																				
User derivation rules	--NONE--																																				
Wired to Wireless Roaming	<input checked="" type="checkbox"/>																																				
SIP authentication role	--NONE--																																				
Device Type Classification	<input checked="" type="checkbox"/>																																				
Enforce DHCP	<input type="checkbox"/>																																				
PAN Firewall Integration	<input type="checkbox"/>																																				
Open SSID radius accounting	<input type="checkbox"/>																																				

- Configure the AAA profile parameters according to your particular use case (refer to [Table 11](#) below for AAA profile parameter details).

Table 11: Configuring AAA Profile Parameters

AAA Profile Parameter	Action/Description	Comments
Initial role	1. Click the Initial Role drop-down list and select a role for unauthenticated users.	The default role for unauthenticated users is logon .
MAC Authentication Default Role	2. Click the MAC Authentication Default Role drop-down list and select the role assigned to the user when the device is MAC authenticated.	The default role for MAC authentication is the guest user role. If derivation rules are present, the role assigned to the client through these rules takes precedence over the default role. NOTE: This feature requires a Policy Enforcement Firewall Next Generation (PEFNG) license.
Download Role from CPPM	3. Enable the Download Role from CPPM option. When you enable this option, the configured ClearPass/RADIUS server provides the role name at user authentication.	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	4. Enable this option to enable the L2-authentication-failthrough mode. <ul style="list-style-type: none"> When this option is enabled, the 802.1X authentication is allowed even if MAC authentication fails. If this option is disabled, 802.1X authentication is not allowed. 	L2-authentication-failthrough mode is disabled by default.
User idle timeout	5. Select the Enable check box to configure the user idle timeout value for this AAA profile. <ol style="list-style-type: none"> Specify the idle timeout value for the client in the number of seconds. 	Enabling this option overrides the global settings configured in the AAA timers. <ul style="list-style-type: none"> If this is disabled, the global settings are applied. Range: 30 to 15300 in multiples of 30 seconds. A value of 0 deletes the user immediately after disassociation from the wireless network.
Max IPv4 for wireless user	6. Specify the number of IPv4 addresses that can be associated to a wireless user. Inter-controller mobility does not support more than two IP addresses per wireless user.	<ul style="list-style-type: none"> Minimum: 1 Maximum: 32 Default: 2

AAA Profile Parameter	Action/Description	Comments
	<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>	
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 User derivation rules drop-down list to specify a user attribute profile from which the user role or VLAN is derived.	
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 SIP authentication role drop-down list.	NOTE: 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 Global Clients table shown in the Monitoring > Network > All WLAN Clients 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. NOTE: 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.	

AAA Profile Parameter	Action/Description	Comments
Open SSID RADIUS Accounting	<p>14. Enable this option to have a Network Access Server (NAS) operate as a client of the RADIUS accounting server.</p> <p>The client is responsible for passing user accounting information to a designated RADIUS accounting server.</p>	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 Apply .	

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 a Dell network, an AP 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 12](#)).

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 12: 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 "Dell-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 85](#)).

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

Figure 71 Virtual AP Profile Configuration Screen

The list of profiles on the left of [Figure 71](#) 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 13](#).

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 13: Basic Virtual AP Profile Parameters

VAP Parameter	Action/Description
General	
Virtual AP enable	1. Select the Virtual AP enable check box to enable or disable the virtual AP. This feature is enabled by default.
VLAN	2. Specify the VLAN(s) into which users are placed in order to obtain an IP address.

VAP Parameter	Action/Description
	<p>To associate that VLAN with the virtual AP profile:</p> <ol style="list-style-type: none"> a. Click the drop-down list to select a configured VLAN. b. Click the Arrow button.
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> <p>3. Click the drop-down list to select one of the following forward modes:</p> <ul style="list-style-type: none"> ● Tunnel: 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. ● Bridge: 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. ● Split-Tunnel: 802.11 frames are either tunneled or bridged, depending on the destination. <p>NOTE: Decrypt-Tunnel: 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>NOTE: Before you configure campus APs in decrypt-tunnel forward mode, you must enable the Control Plane Security feature on the mobility controller.</p>
RF	
Allowed band	<p>4. Specify the band on which to use the virtual AP:</p> <ul style="list-style-type: none"> ● a—802.11a band only (5 GHz) ● g—802.11b/g band only (2.4 GHz) ● all—Both 802.11a and 802.11b/g bands (5 GHz and 2.4 GHz) <p>The default band setting is all.</p>
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"> ● This feature supports both campus APs and remote APs that have a virtual AP profile set to tunnel, split-tunnel, or bridge forwarding mode. ● This feature is disabled by default, and must be enabled in a virtual AP profile.
Steering Mode	<p>6. Specify the Band Steering mode:</p> <ul style="list-style-type: none"> ● Force-5GHz: When the AP is configured in force-5GHz band steering mode, the

VAP Parameter	Action/Description
	<p>AP tries to force 5Ghz-capable APs to use that radio band.</p> <ul style="list-style-type: none"> • Prefer-5GHz (Default): If you configure the AP to use Prefer-5GHz 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. • Balance-bands: The AP balances the clients across the two radios to best utilize the available 2.4G bandwidth.
Broadcast/Multicast	
Dynamic Multicast Optimization (DMO)	7. Select this check box to enable Dynamic Multicast Optimization . This parameter is disabled by default, and cannot be enabled without the Policy Enforcement Firewall Next Generation (PEFNG) license.
Drop Broadcast and Multicast	<p>8. Select the Drop Broadcast and Multicast check box to filter out broadcast and multicast traffic in the air.</p> <p>NOTE: 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>IMPORTANT: If you enable this option, you must also enable the Broadcast-Filter ARP parameter on the virtual AP profile to prevent ARP requests from being dropped. You can enable this parameter by checking the Convert Broadcast ARP requests to unicast check box as described in the following parameter (Convert Broadcast ARP requests to unicast).</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.</p> <p>You can check the status of this option using the show ap active and the show datapath tunnel commands. The output displays the letter a in the Flags column.</p> <p>The Convert Broadcast ARP requests to unicast option includes the additional functionality of a broadcast-filter all parameter, where DHCP response frames are sent as unicast to the corresponding client.</p> <p>NOTE: This option, when enabled, can impact DHCP discover packets, requested packets for clients that are behind a wireless bridge, and virtual clients on VMware devices.</p> <ul style="list-style-type: none"> • To resolve this issue and allow clients that are behind a wireless bridge or VMware devices to receive an IP address, disable this option. <p>This parameter is enabled by default.</p>
	10. When finished specifying the Virtual AP profile settings, click Apply

This completes the configuration for the Virtual AP Profile.

Configuring W-ClearPass as an RFC 3576 (CoA) Server

This section contains the following information:

- [About the CoA Server](#)

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

About the CoA Server

This section describes how to configure the W-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 W-ClearPass Server as a CoA Server

To configure the W-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 W-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 W-ClearPass server’s IP address is not already listed in the list of RFC 3576 servers, enter the IP address of the W-ClearPass server in the **Add** text box, then click **Add**.

Figure 72 Adding an RFC 3576 Server

RFC 3576 Server	
Instance	Actions
10.10.110.20	Add

The IP address of the W-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 73 Setting 3576 Server Parameters

RFC 3576 Server > 10.162.114.23

Show Reference Save As Reset

Key
Retype:
Radsec	<input 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 W-ClearPass server, the values for RADIUS key configured on the mobility controller and the RADIUS shared secret configured on the W-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.

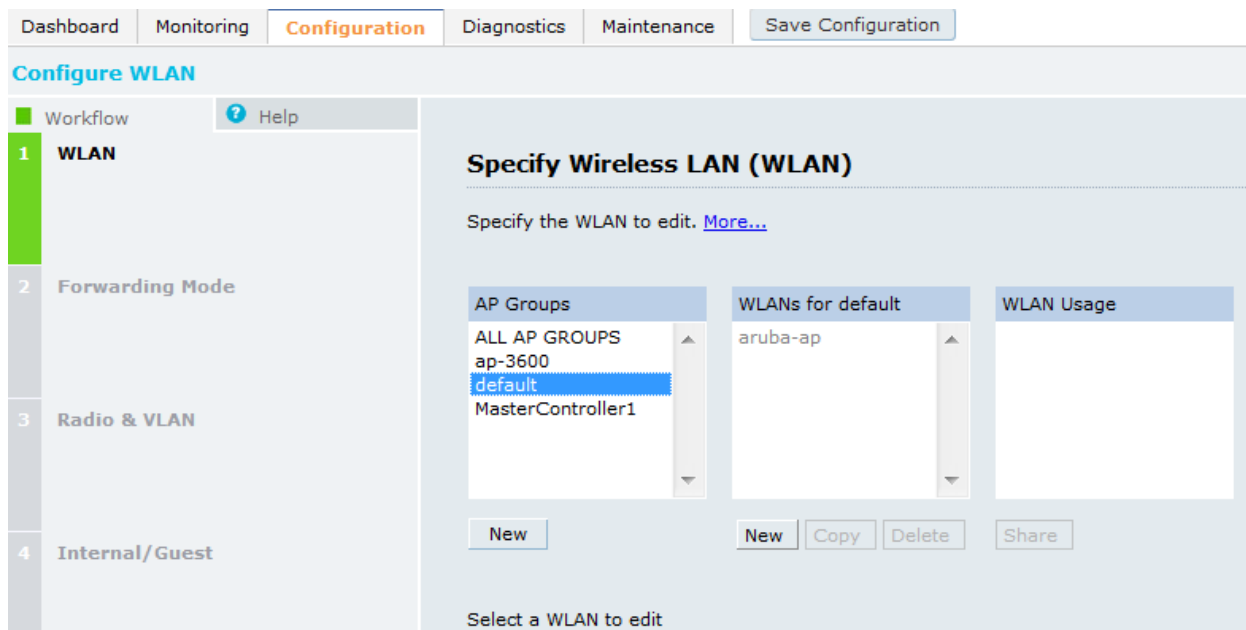
Adding an SSID to the Mobility Controller

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:

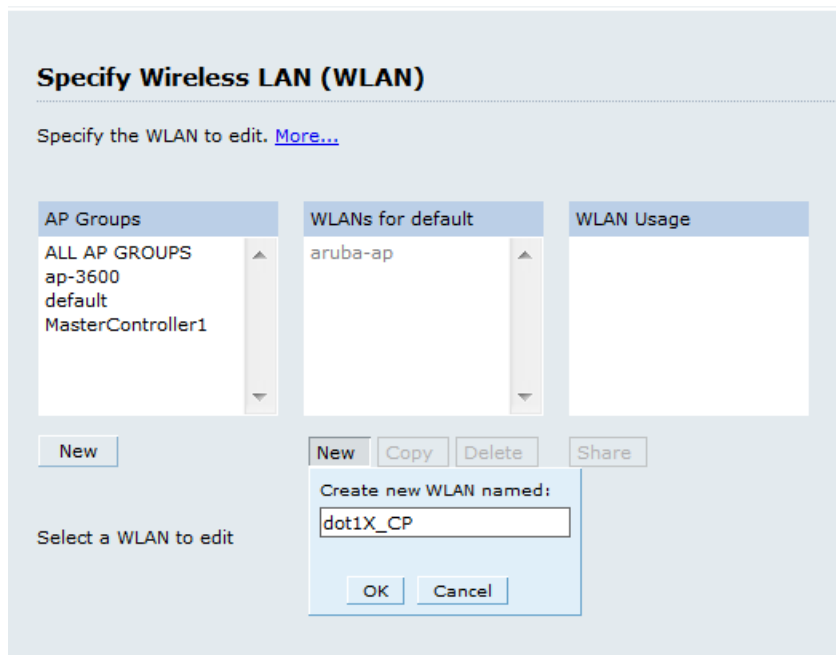
1. On the mobility controller, navigate to **Configuration > WIZARDS > Campus WLAN**.
The **Configure WLAN** wizard opens.

Figure 74 *Specifying the Wireless LAN*



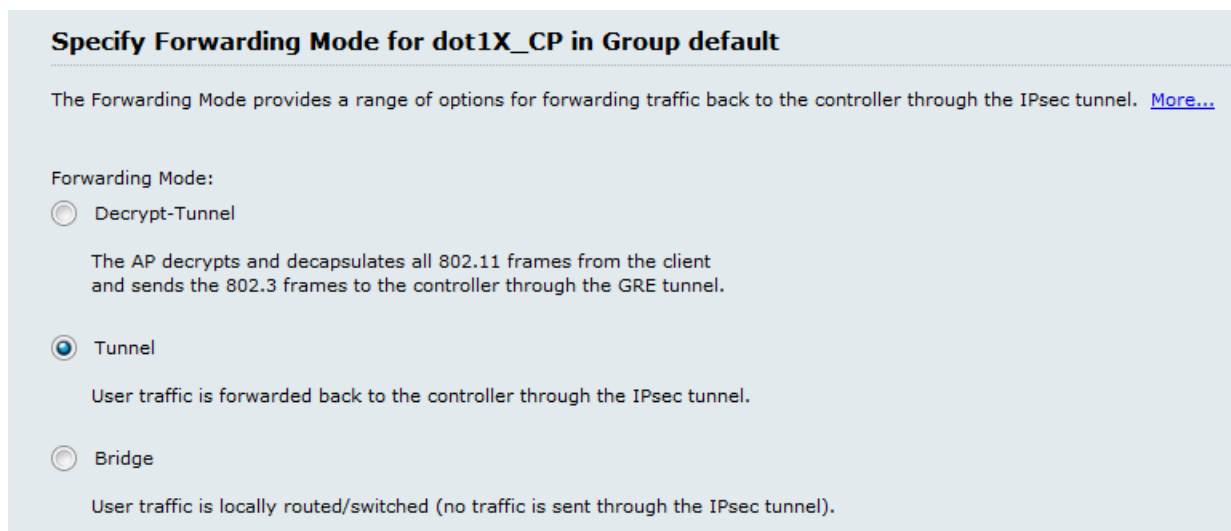
2. From the **AP Groups** pane, select the appropriate AP group, or click **New** to create a new AP group.
3. From the **WLANs for <name>** pane, select the Wireless LAN you wish to use, or click **New** to create a new Wireless LAN.
4. In the **Create New WLAN Named** dialog, enter the name of the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

Figure 75 *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 76 *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.
- Click **Next**.
The **Radio Type and VLAN** configuration screen appears.

Figure 77 Specifying Radio Type and VLAN ID

Specify Radio Type and VLAN for dot1X_CP in Group default

Specify the radio type on which this WLAN is available, as well as the VLAN in which users connecting to this WLAN are to be placed by default. Note: you can override the VLAN specified below by configuring per-role VLANs in Step 8. [More...](#)

Radio Type:

Broadcast SSID:

VLAN:

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 78 Specifying the WLAN Usage Scenario

Specify Usage Scenario for dot1X_CP in Group default

Guest WLANs allow guests to access the Internet, while blocking access to the internal network. Guest WLANs are not encrypted, and at most require Web-based authentication. Internal WLANs typically employ encryption and stronger layer 2 authentication. [More...](#)

Is this WLAN intended for internal use or for use by guests?

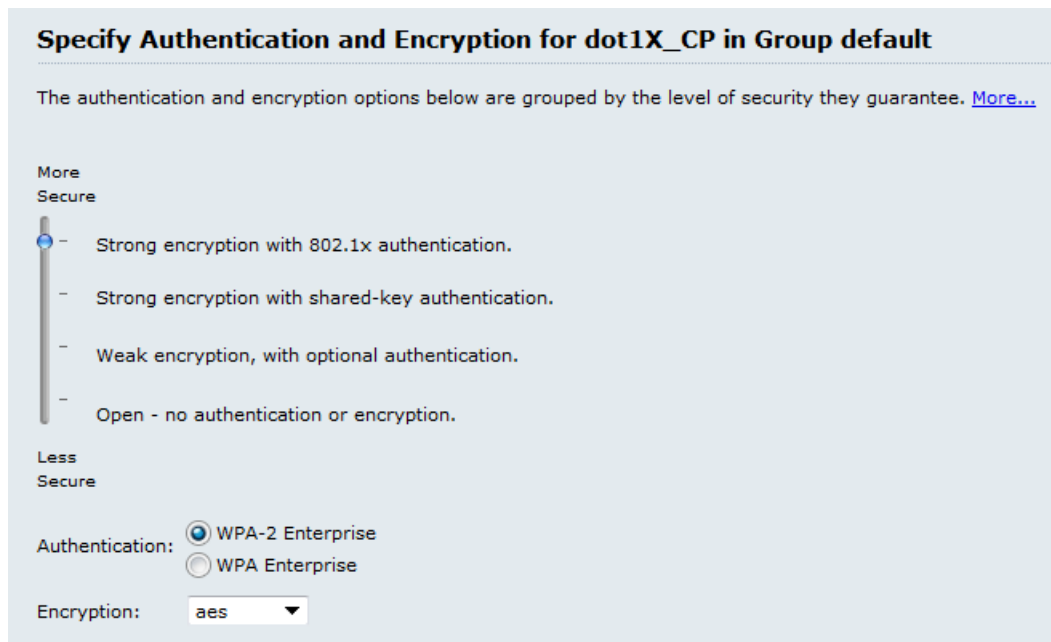
Internal

Guest

- 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 appears.

Figure 79 *Setting Up Authentication and Encryption*



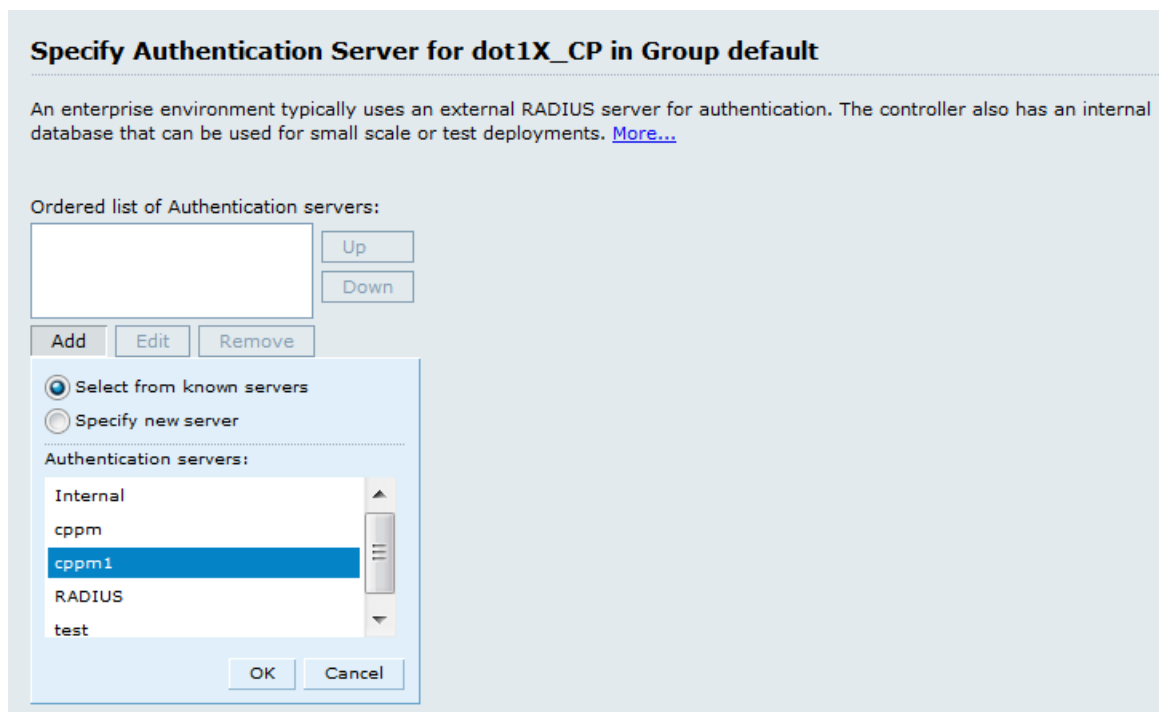
10. For this step, do the following:

- 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 80 *Specifying the Authentication Server for the WLAN*



11. To specify an existing W-ClearPass/RADIUS authentication server, click **Add**.

- a. Choose **Select from known servers**.
- b. Scroll to select the W-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 82](#)).

12. To specify a new W-ClearPass/RADIUS authentication server, click **Add**.

- a. Choose **Specify new server**.

The following dialog is displayed:

Figure 81 *Specifying a New Authentication Server*

- b. Populate the Authentication Server parameters as described in [Table 14](#).

Table 14: *New SSID Authentication Server Parameters*

Parameter	Action/Description
Server type	1. Choose the default server type: RADIUS .
Name	2. Enter the name of the W-ClearPass Policy Manager server.
IP address	3. Enter the IP address of the W-ClearPass Policy Manager server.
Auth port	4. Specify the authentication port on the RADIUS/Policy Manager server. <ul style="list-style-type: none"> ● Range: 1 to 65535 ● Default: 1812

Parameter	Action/Description
Acct port	5. Specify the accounting port on the RADIUS/Policy Manager server. <ul style="list-style-type: none"> Range: 1 to 65535 Default: 1813
Shared Key	6. Specify the RADIUS Shared Secret for the W-ClearPassPolicy Manager server. NOTE: Make sure that the value of the Key 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 Table 10).

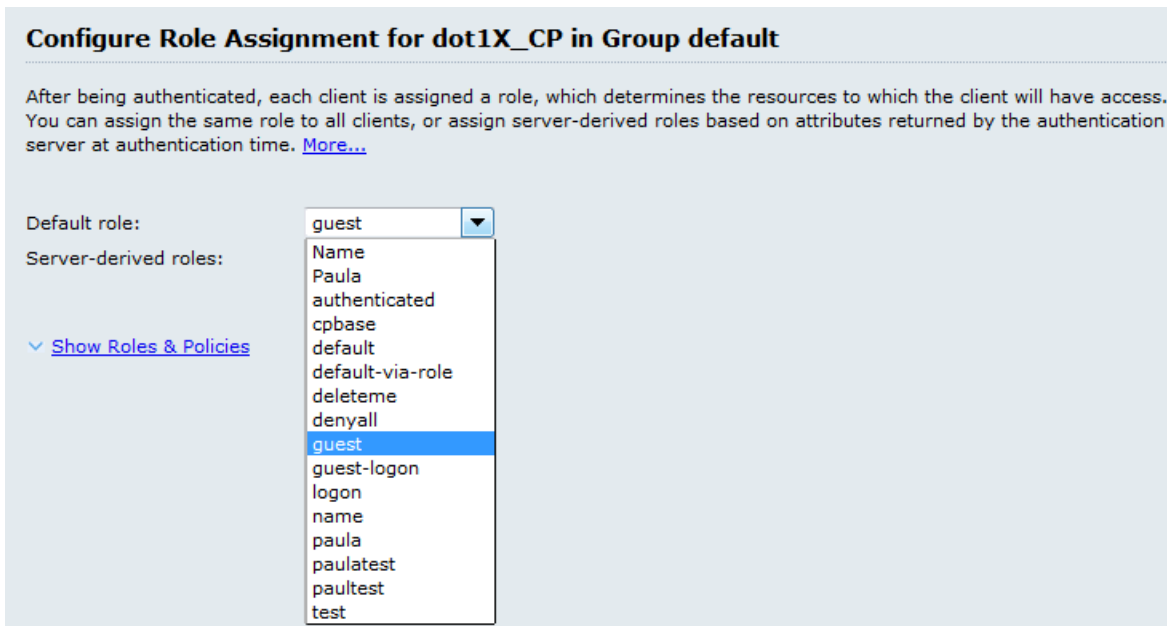
c. When finished, click **OK**.

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

d. Click **Next**.

The **Configure Role Assignment** screen appears.

Figure 82 *Configuring the Role Assignment*



- 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 W-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.

This chapter describes the required steps to integrate W-ClearPass Policy Manager and Microsoft Active Directory. For some use cases, it's required that W-ClearPass is joined to 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 W-ClearPass to Active Directory is optional.

This chapter includes the following information:

- [Joining a W-ClearPass Server to an Active Directory Domain](#)
- [Adding Active Directory as an Authentication Source to W-ClearPass](#)
- [Obtaining and Installing a Signed Certificate From Active Directory](#)
- [Manually Testing Login Credentials Against Active Directory](#)

Joining a W-ClearPass Server to an Active Directory Domain

This section contains the following information:

- [Introduction](#)
- [Confirming the Date and Time Are in Sync](#)
- [Joining an Active Directory Domain](#)
- [About the Authentication Source and the Authorization Process](#)
- [Manually Specifying Active Directory Domain Controllers for Authentication](#)
- [Disassociating a W-ClearPass Server From an Active Directory Domain](#)

Introduction

The first task in preparing W-ClearPass for Active Directory® (AD) authentication via EAP-PEAP-CHAP-v2 is to join the W-ClearPass server to an Active Directory domain. Joining W-ClearPass Policy Manager to an Active Directory domain allows you to authenticate users and computers that are members of an Active Directory domain.

Joining W-ClearPass Policy Manager to an Active Directory domain creates a computer account for the W-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 their own Active Directory credentials.

A one-time procedure to join W-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 W-ClearPass need to join Active Directory to perform EAP-PEAP-MS-CHAPv2 authentication for 802.1x? W-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 W-ClearPass to each of these untrusting forests or domains.



You do not need to join W-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.

Confirming the Date and Time Are in Sync

Assuming that this W-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 W-ClearPass server and the Active Directory domain controller that you will use for the join domain operation.

1. In W-ClearPass Policy Manager, navigate to **Administration > Server Manager > Server Configuration**. The **Server Configuration** screen appears:

Figure 83 *Server Configuration Screen*

Administration » Server Manager » Server Configuration

Server Configuration

- [Set Date & Time](#)
- [Change Cluster Password](#)
- [Manage Policy Manager Zones](#)
- [NetEvents Targets](#)
- [Virtual IP Settings](#)
- [Clear Machine Authentication Cache](#)
- [Make Subscriber](#)
- [Cluster-Wide Parameters](#)

Publisher Server: manisha-200 [10.2.50.200]

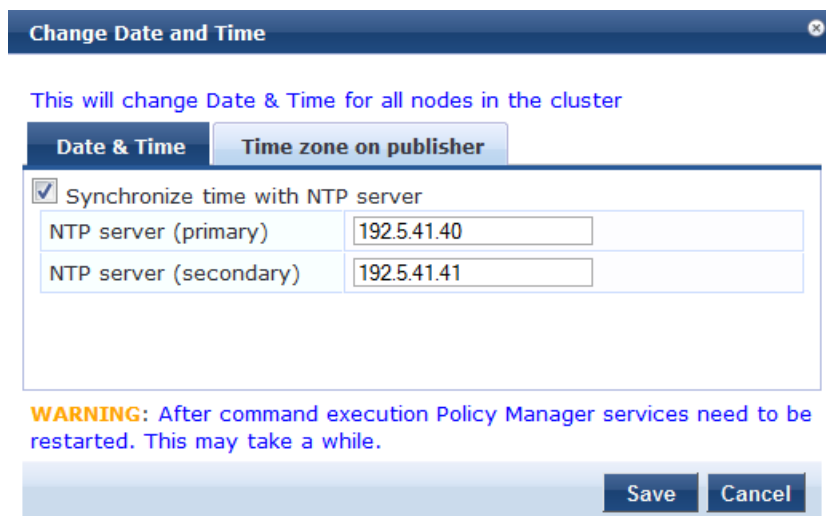
#	Server Name ▲	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	manisha-200	10.2.50.200	-	default	Enabled	Enabled	-

Showing 1-1 of 1

[Collect Logs](#)
[Backup](#)
[Restore](#)
[Cleanup](#)
[Shutdown](#)
[Reboot](#)

2. From the **Server Configuration** screen, click **Set Date and Time**. The **Change Date and Time** dialog appears.

Figure 84 *Confirming NTP Server Synchronization*



Change Date and Time

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

Date & Time Time zone on publisher

Synchronize time with NTP server

NTP server (primary)	192.5.41.40
NTP server (secondary)	192.5.41.41

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

Save Cancel

To synchronize with a Network Time Protocol server, the **Synchronize time with NTP server** check box must be enabled. No more than two NTP servers can be specified.

In the example shown in [Figure 84](#), the W-ClearPass Policy Manager server is synchronized to two NTP servers on the Internet.

3. Return to the **Server Configuration** page by clicking **Cancel**.
4. Compare the clock time displayed at the bottom of the W-ClearPass **Server Configuration** page against the clock time on the Active Directory server.



The maximum allowed clock skew between the W-ClearPass server and the Active Directory server is five minutes.

5. If the time on the two systems doesn't exceed the clock skew limit, then proceed.

Joining an Active Directory Domain

To join a W-ClearPass server to an Active Directory domain:

1. In the **Server Configuration** screen, click the **name of the W-ClearPass server** that you want to join to the domain.
The **Server Configuration** screen for the selected server opens.

Figure 85 Server Configuration Screen for Selected W-ClearPass Server

The screenshot shows the 'Server Configuration' interface with the following details:

- System** | **Services Control** | **Service Parameters** | **System Monitoring** | **Network** | **FIPS**
- Hostname: CP-66-200
- FQDN: [Empty]
- Policy Manager Zone: default (with a link to 'Manage Policy Manager Zones')
- Enable Profile: Enable this server for endpoint classification
- Enable Performance Monitoring Display: Enable this server for performance monitoring display
- Insight Setting: Enable Insight Enable as Insight Master
Current Master: manisha-200(10. [Redacted])
- Enable Ingress Events Processing: Enable Ingress Events processing on this server
- Span Port: -- None --

	IPv4	IPv6	Action
Management Port	IP Address	10. [Redacted]	<input type="button" value="Configure"/>
	Subnet Mask	255.255.255.0	
	Default Gateway	10. [Redacted]	
Data/External Port	IP Address		<input type="button" value="Configure"/>
	Subnet Mask		
	Default Gateway		
DNS Settings	Primary	10. [Redacted]	<input type="button" value="Configure"/>
	Secondary	10. [Redacted]	
	Tertiary		

AD Domains: Policy Manager is not part of any domain. Join to domain here.

[Back to Server Configuration](#)

You can now join the Active Directory domain.

2. Click **Join AD Domain**.

The **Join AD Domain** dialog opens.

Figure 86 Join AD Domain Dialog

The 'Join AD Domain' dialog contains the following elements:

- Enter the FQDN of the controller and the short (NETBIOS) name for the domain:
- Domain Controller: [Text Input]
- NetBIOS Name: [Text Input]
- 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: [Text Input]
- Password: [Text Input]
-

3. **Domain Controller:** Enter the Fully Qualified Domain Name (FQDN) of the domain controller, then press **Tab**.



Note that the primary DNS server IP address (as shown in [Figure 85](#)) is also the IP address of the Active Directory domain controller.

The following message is displayed:
Trying to determine the NetBIOS name...

W-ClearPass searches for the NetBIOS name for the domain.



NetBIOS is another term for the short domain name, or the NT4 domain name, also known as the pre-Windows 2000 domain name.

[Figure 87](#) shows that W-ClearPass found the NetBIOS domain name and populated the **NetBIOS Name** field with the correct name.

Figure 87 *Entering the Domain Controller FQDN*

4. **In case of a controller name conflict:**

- a. **Use specified Domain Controller:** Accept the default setting.
- b. **Use default domain admin user [Administrator]:** Accept the default setting.



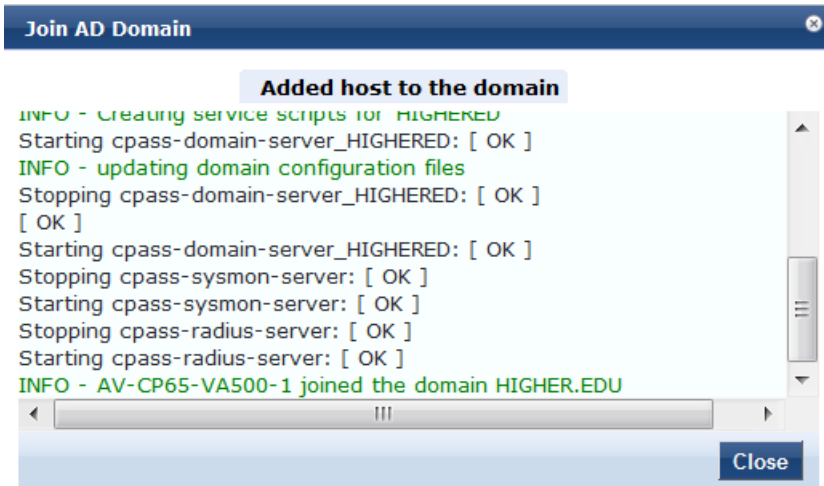
In a production environment, it is likely that an Administrative username that has permissions to join machines to the domain would be used for the default domain admin user. In that case, 1) disable (uncheck) the **Use default domain admin user [Administrator]** check box and 2) enter the Administrative username and password in the fields provided.

- c. **Password:** Enter the password for the user account that will join W-ClearPass with the domain, then 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 88 W-ClearPass Server Added to the Active Directory Domain

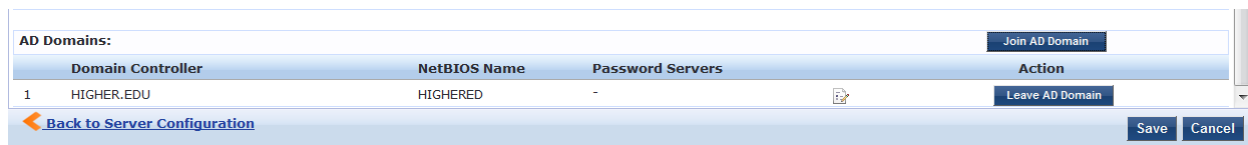


The **Join AD Domain** status screen indicates that the services have restarted. As shown in [Figure 88](#), the final INFO line states that the selected W-ClearPass server joined the domain.

5. Click **Close**.

You return to the **Server Configuration** page, and it now shows that the W-ClearPass server is joined to the domain.

Figure 89 W-ClearPass Server Joined to Domain



Now that the W-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 NTLM authentication process, W-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 W-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 Specifying Active Directory Domain Controllers for Authentication](#).

If you do not specify this list of domain controllers, all available domain controllers obtained from DNS will be used for authentication.

Manually Specifying Active Directory Domain Controllers for Authentication

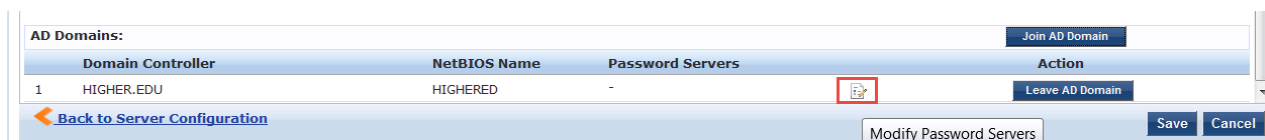
To manually specify Active Directory domain controllers for authentication:

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. Select the W-ClearPass server name.

The **Server Configuration** page for the selected server opens by default on the **System** tab.

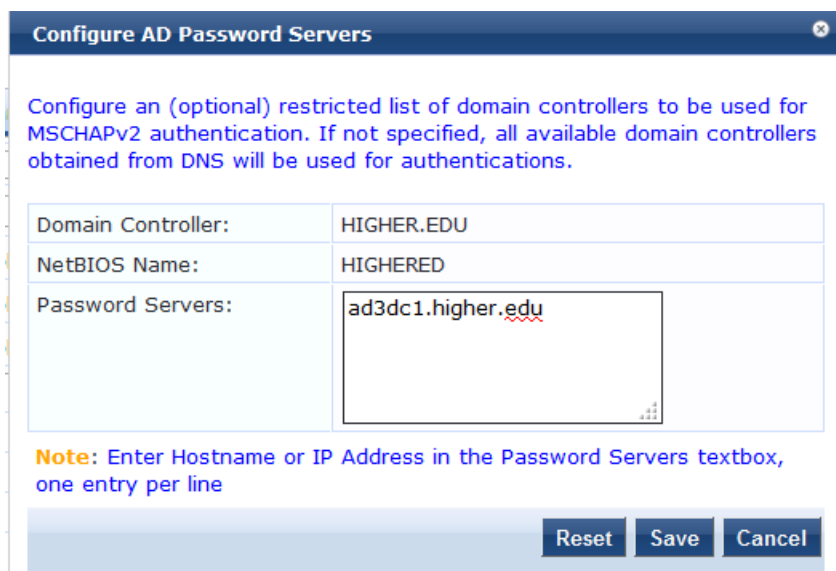
3. Click the **Modify Password Servers** icon (located at the bottom of the **System** page).

Figure 90 Location of Modify Password Servers Icon



The **Configure AD Passwords Servers** screen appears.

Figure 91 Configuring Active Directory Password Servers



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 W-ClearPass Server From an Active Directory Domain

If a W-ClearPass Policy Manager server is already part of multiple Active Directory domains, follow this procedure to disassociate this W-ClearPass appliance from an Active Directory domain.

To disassociate a W-ClearPass server from an Active Directory domain:

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. Select the name of the W-ClearPass server that you want to disassociate from the domain.
3. Click **Leave AD Domain**.

The **Leave AD Domain** dialog opens.

Figure 92 Leave AD Domain Dialog

Leave AD Domain

Domain Controller: HIGHERED

Leave domain even if AD is Down

Use default domain admin user [Administrator]

Username: []

Password: []

Buttons: Leave, Cancel

4. Enter the Administrator account password.



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.

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 W-ClearPass server is no longer listed in the AD Domains section.

7. Click **Save**.

Adding Active Directory as an Authentication Source to W-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 W-ClearPass to the domain, add an authentication source to W-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 W-ClearPass. This allows W-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 W-ClearPass Policy Manager to the Active Directory domain. Joining the Active Directory domain is necessary in order for W-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 W-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 W-ClearPass only serves for authorization and not authentication. When authenticating users via Captive Portal, the authentication source created in W-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 W-ClearPass runs. When a user is authenticating, they give W-ClearPass their username. After authentication is successfully completed, W-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 a 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.

The 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.

Active Directory needs to know which group each user who is trying to authenticate is a member of. This allows W-ClearPass to do *enforcement*, which is the process of determining what each user will be allowed to do on the network.

Additional Enforcement Information

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 the W-ClearPass Policy Manager, navigate to **Configuration > Authentication > Sources**.

The following screen appears:

Figure 93 Authentication Sources Screen

Configuration » Authentication » Sources

Authentication Sources

[+ Add](#)
[Import](#)
[Export All](#)

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

#	Name ▲	Type	Description
1.	[Admin User Repository]	Local SQL DB	Authenticate users against Policy Manager admin user database
2.	[Blacklist User Repository]	Local SQL DB	Blacklist database with users who have exceeded bandwidth or session related limits
3.	[Endpoints Repository]	Local SQL DB	Authenticate endpoints against Policy Manager local database
4.	[Guest Device Repository]	Local SQL DB	Authenticate guest devices against Policy Manager local database
5.	[Guest User Repository]	Local SQL DB	Authenticate guest users against Policy Manager local database
6.	[Insight Repository]	Local SQL DB	Insight database with session information for users and devices
7.	[Local User Repository]	Local SQL DB	Authenticate users against Policy Manager local user database
8.	[Onboard Devices Repository]	Local SQL DB	Authenticate Onboard devices against Policy Manager local database
9.	[Social Login Repository]	Local SQL DB	Authenticate users against Policy Manager social login database
10.	[Time Source]	Local SQL DB	Authorization source for implementing various time functions

Showing 1-10 of 10 [Copy](#) [Export](#) [Delete](#)

2. Click **Add**.

General Page

The Authentication Sources **General** page appears.

Figure 94 Authentication Sources General Page

Configuration » Authentication » Sources » Add

Authentication Sources

General	Primary	Attributes	Summary
Name:	<input type="text" value="ad1dc1"/>		
Description:	<input type="text"/>		
Type:	Active Directory ▼		
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes		
Authorization Sources:	<input type="text" value="-- Select --"/>		<input type="button" value="Remove"/> <input type="button" value="View Details"/>
Server Timeout:	<input type="text" value="10"/> seconds		
Cache Timeout:	<input type="text" value="36000"/> seconds		
Backup Servers Priority:	<input type="text"/>		<input type="button" value="Move Up"/> <input type="button" value="Move Down"/> <input type="button" value="Add Backup"/> <input type="button" value="Remove"/>

3. Enter the values for these parameters as described in [Table 15](#).

Table 15: General Parameters for an AD Authentication Source

Parameter	Action/Description
Name	1. Enter the name of the Active Directory authentication source.
Description	2. Provide the additional information that helps to identify the Active Directory authentication source.
Type	3. If not already selected, select Active Directory .
Use for Authorization	When <i>Use for Authorization</i> is enabled, W-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>4. Select a previously configured authentication source from the drop-down list.</p> <p>5. To add authentication source to the list of authorization sources, click Add. To remove the authentication source from the list, click Remove.</p> <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>

Parameter	Action/Description
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	<p>Policy Manager caches attributes fetched for an authenticating entity. This parameter controls the duration in number of seconds for which the attributes are cached.</p>
Backup Servers Priority	<ol style="list-style-type: none"> To add a backup server, click Add Backup. The Backup 1 tab appears. The Primary page parameters are prepopulated in the Backup 1 page. To complete the configuration for the backup server, specify the hostname for the backup server. <ul style="list-style-type: none"> To remove a backup server, select the server name and click Remove. To change the server priority of the backup servers, select Move Up or Move Down. <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>NOTE: Dell recommends setting up one or more backup servers.</p>

- When satisfied with these settings, click **Next**.
The Authentication Sources **Primary** page opens.

Primary Page

Figure 95 Primary Page: Active Directory Authentication Source

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
Connection Details			
Hostname:	<input type="text" value="ad1dc2"/>		
Connection Security:	<input type="text" value="AD over SSL"/>		
Port:	<input type="text" value="636"/> (For secure connection, use 636)		
Verify Server Certificate:	<input checked="" type="checkbox"/> Enable to verify Server Certificate for secure connection		
Bind DN:	<input type="text"/> (e.g. administrator@example.com OR cn=administrator,cn=users,dc=example,dc=com)		
Bind Password:	<input type="password"/>		
NetBIOS Domain Name:	<input type="text"/>		
Base DN:	<input type="text"/>		Search Base Dn
Search Scope:	<input type="text" value="SubTree Search"/>		
LDAP Referrals:	<input type="checkbox"/> Follow referrals		
Bind User:	<input checked="" type="checkbox"/> Allow bind using user password		
User Certificate :	<input type="text" value="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 16](#).

Table 16: Primary Parameters for an Active Directory Authentication Source

Parameter	Action/Description
Hostname	<p>1. 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). W-ClearPass uses LDAP to talk to the domain controller.</p>
Connection Security	<p>2. Set Connection Security to: AD over SSL.</p> <p>This enables the secure sockets layer (SSL) cryptographic protocol to connect to your Active Directory. Selecting AD over SSL automatically populates the <i>Port</i> field to 636.</p> <p>NOTE: In a production environment, security is a concern because when W-ClearPass binds to an LDAP server, it submits the username and password for that account over the network under clear text unless you protect it using Connection Security and set the port to 636.</p> <p>NOTE: 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 Importing the Root CA Files to the Certificate Trust List.</p>
Port	<p>3. 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"> • Default port for LDAP: 389 • Default port for LDAP over SSL: 636 <p>When you set the <i>Connection Security</i> field to AD over SSL, this port is automatically set to 636.</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"> • Default port without SSL: 3268 • Default port with SSL: 3269
Verify Server Certificate	<p>4. Enable this option to verify the Server Certificate for a secure connection.</p>
Bind DN	<p>5. 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 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>NOTE: 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"> For a single domain Active Directory Domain Service, the Bind DN entry must be located in the same branch and below the Base DN. 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. <p>W-ClearPass fills in the domain portion of the Bind DN.</p> <p>6. Specify the username.</p> <p>W-ClearPass also populates the <i>Base DN</i>, and the <i>NetBIOS Domain Name</i> fields.</p> <p>For related information, see About the Bind Operation.</p>
Bind Password	<p>This is the text box for the Active Directory password for the account that can search for users.</p> <p>7. Enter the Bind Password.</p> <p>NOTE: 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"> 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: DC=mycompany,DC=com <p>Active Directory starts from this DN to create master lists from which you can later filter out individual users and groups.</p> <p>NOTE: The Base DN value that is automatically populated in this instance is <i>not</i> the best practice Base DN value.</p> <p>Dell 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> <p>8. To browse the LDAP directory hierarchy, click Search Base DN.</p> <p>9. The LDAP Browser opens.</p> <p>10. Navigate to the DN you want to use as the Base DN.</p> <p>11. Click on the appropriate node in the tree structure to select it as a Base DN.</p> <ul style="list-style-type: none"> For a multi-domain Active Directory Domain Service (AD DS) forest, the appropriate action is to leave the Base DN text box blank. <p>NOTE: 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 Search Base DN.</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>12. Specify the search scope you wish to apply.</p> <ul style="list-style-type: none"> Subtree Search: Searches every object and sub-object in the LDAP directory. One-Level Search: Looks directly under the Base DN.

Parameter	Action/Description
	<ul style="list-style-type: none"> Base Object: Searches any object under the Base DN.
LDAP Referrals	Dell does <i>not</i> recommend 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 Allow bind using user password 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.

13. When satisfied with the Authentication Sources **Primary** page settings, click **Next**.

The Active Directory **Attributes** page opens.

Active Directory > Attributes Page

Figure 96 Active Directory Default Attributes

Configuration » Authentication » Sources » Add

Authentication Sources

General	Primary	Attributes	Summary
Specify filter queries used to fetch authentication and authorization attributes			
Filter Name	Attribute Name	Alias Name	Enabled As
1. Authentication	dn	UserDN	-
	department	Department	-
	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	-

[Add More Filters](#)

The **Attributes** dialog defines the Active Directory or LDAP Directory query filters and the attributes to be fetched by using those filters.

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 W-ClearPass Deployments](#)
- [How 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 W-ClearPass](#)

About Certificates in W-ClearPass Deployments

A certificate is a file that makes it possible for network devices to communicate with each other securely. For example, in W-ClearPass deployments, certificates are provided for all devices involved in authentication, such as client laptops, smart phones, Mobility controllers, Mobility Access Switches, W-ClearPass Policy Manager servers, and so on.

How do certificates help you to 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 W-ClearPass deployments:

- When using HTTPS to manage network devices such as mobility controllers, mobility access switches, or W-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 W-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 W-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.

How 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 a server certificate into the W-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 97](#) shows an example of the Create Certificate Signing Request page, followed by descriptions of each parameter (see [Table 17](#)).

To create a Certificate Signing Request:

1. In W-ClearPass, navigate to **Administration > Certificates > Server Certificates**.
2. Select the **Create Certificate Signing Request** link.

Figure 97 Create Certificate Signing Request Dialog

3. Enter the information for each of the required parameters as described in [Table 17](#).

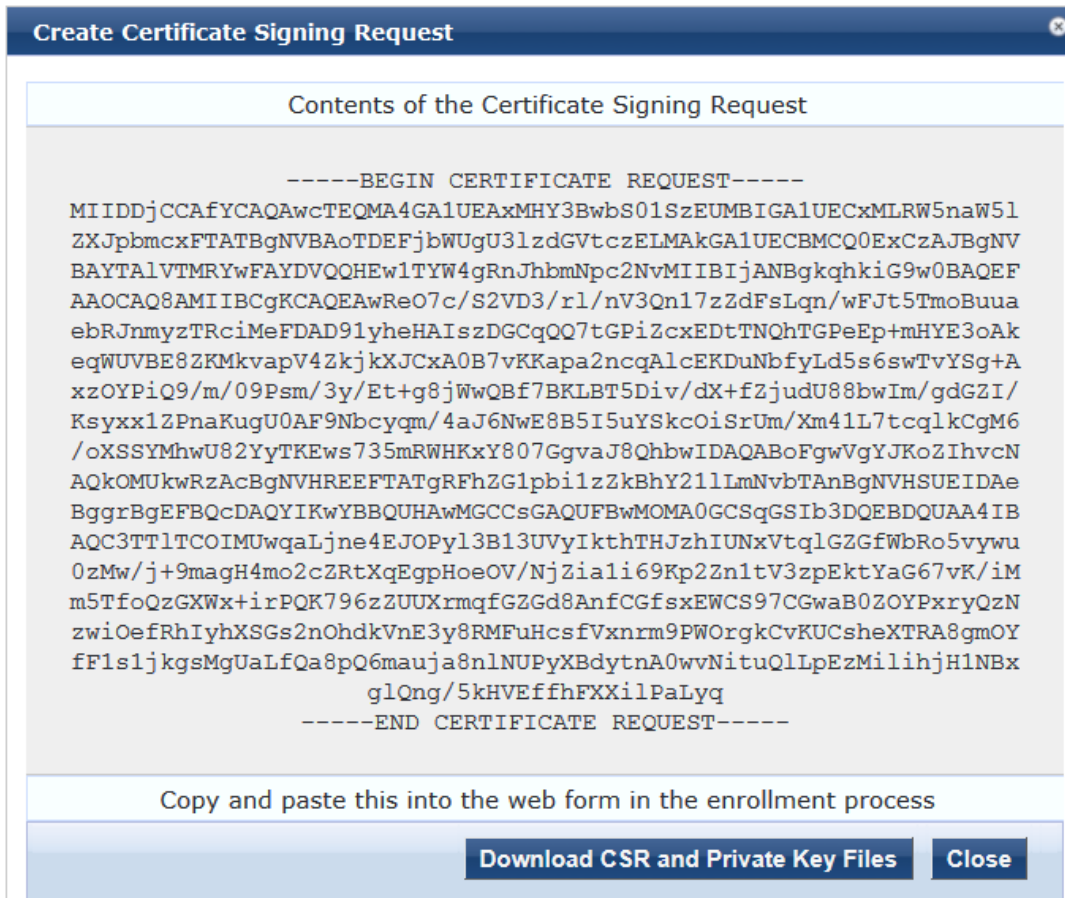
Table 17: Parameters for Creating a Certificate Signing Request

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)	Specify the name of the state, country, and/or another location. These fields are optional
State (ST)	
Country (C)	
Subject Alternate Name (SAN)	Specify the alternative names for the specified Common Name. NOTE: Specify the SAN in the following formats: <ul style="list-style-type: none"> ● email: <i>email_address</i> ● URI: <i>url</i>

Parameter	Action/Description
	<ul style="list-style-type: none"> • IP: <i>ip_address</i> • dns: <i>dns_name</i> • rid: <i>id</i> <p>This field is optional.</p>
Private Key Password	1. Enter the private key password, then reenter it to verify the password.
Private Key Type	<p>2. Select the length for the generated private key types from the following options:</p> <ul style="list-style-type: none"> • 1024-bit RSA • 2048-bit RSA • 4096-bit RSA • X9.62/SECG curve over a 256 bit prime field • NIST/SECG curve over a 384 bit prime field <p>The default private key type is 2048-bit RSA.</p>
Digest Algorithm	<p>3. Select one of the following message digest algorithms:</p> <ul style="list-style-type: none"> • MD5 • SHA-1 • SHA-224 • SHA-256 • SHA-384 • SHA-512 <p>NOTE: The MD5 algorithm is not available in FIPS mode.</p>

4. When satisfied with the certificate signing request parameter settings, click **Submit**.
The **Certificate Signing Request** is generated and displayed (see [Figure 98](#)).

Figure 98 Displayed View of the 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 113](#).
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 W-ClearPass *before* starting this operation.

To import the root CA files into the W-ClearPass server Certificate Trusted List:

1. Get all of 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 W-ClearPass Policy Manager, navigate to **Administration > Certificates > Trust List**.

Figure 99 Certificate Trust List

Administration » Certificates » Trust List

Certificate Trust List + Add

Filter: Subject contains [] + Go Clear Filter Show 10 records

#	Subject	Validity	Enabled
1.	<input type="checkbox"/> C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA	valid	Disabled
2.	<input type="checkbox"/> C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Universal CA, CN=TC TrustCenter Universal CA I	valid	Disabled
3.	<input type="checkbox"/> C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High-Assurance Secure Server CA	valid	Disabled
4.	<input type="checkbox"/> CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	valid	Enabled
5.	<input type="checkbox"/> CN=InCommon Server CA, OU=InCommon, O=Internet2, C=US	valid	Enabled
6.	<input checked="" type="checkbox"/> CN=ns-ISCA-CA, DC=ns, DC=arubatac, DC=us	valid	Enabled
7.	<input type="checkbox"/> CN=ns-RCA-CA, DC=ns, DC=arubatac, DC=us	valid	Enabled
8.	<input type="checkbox"/> C=PL, O=Unizeto Sp. z o.o., CN=Certum CA	valid	Disabled
9.	<input type="checkbox"/> C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root	valid	Enabled
10.	<input type="checkbox"/> C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	valid	Disabled

Showing 1-10 of 43 Delete

3. 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 100 New Root CA File(s) Added to the Certificate Trust List

aruba NETWORKS ClearPass Policy Manager SUPPORT | HELP admin (Super Adm)

Administration » Certificates » Trust List

Certificate Trust List + Add

1 Certificate(s) added to the trust list

Filter: Subject contains [] + Go Clear Filter Show 10

#	Subject	Validity	Enabled
1.	<input type="checkbox"/> C=BE, O=GlobalSign nv-sa, OU=Root CA, CN=GlobalSign Root CA	valid	Disabled
2.	<input type="checkbox"/> C=DE, O=TC TrustCenter GmbH, OU=TC TrustCenter Universal CA, CN=TC TrustCenter Universal CA I	valid	Disabled
3.	<input type="checkbox"/> C=GB, ST=Greater Manchester, L=Salford, O=COMODO CA Limited, CN=COMODO High-Assurance Secure Server CA	valid	Disabled
4.	<input type="checkbox"/> CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE	valid	Enabled
5.	<input type="checkbox"/> CN=InCommon Server CA, OU=InCommon, O=Internet2, C=US	valid	Enabled
6.	<input type="checkbox"/> CN=ns-ISCA-CA, DC=ns, DC=arubatac, DC=us	valid	Enabled
7.	<input type="checkbox"/> CN=ns-RCA-CA, DC=ns, DC=arubatac, DC=us	valid	Enabled
8.	<input type="checkbox"/> C=PL, O=Unizeto Sp. z o.o., CN=Certum CA	valid	Disabled
9.	<input type="checkbox"/> C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA Root	valid	Enabled
10.	<input type="checkbox"/> C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert Global Root CA	valid	Disabled

Showing 1-10 of 43 Delete

4. Make sure the Enabled column for the newly added certificate says *Enabled*, which is the correct status when you successfully import a certificate manually.
5. 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 109](#).

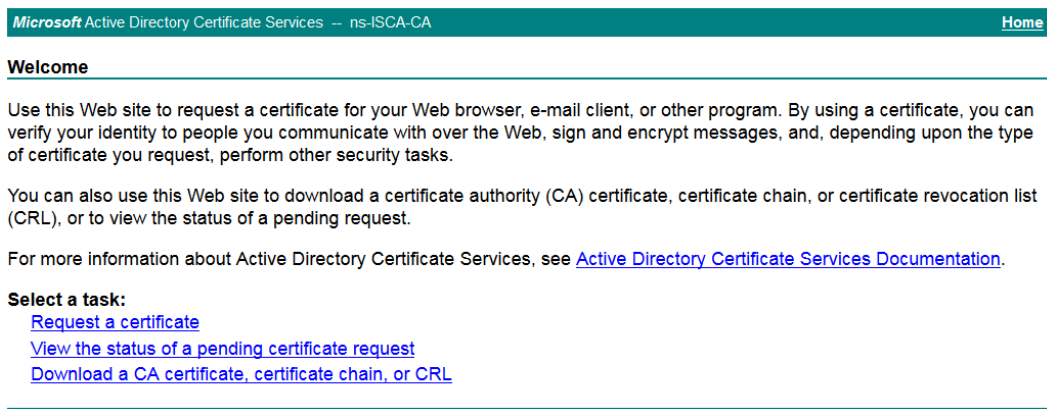
Also note the location where you saved the Certificate Signing Request and the private key password files, as you will need to retrieve these items to complete this operation.



To obtain a signed certificate from Active Directory:

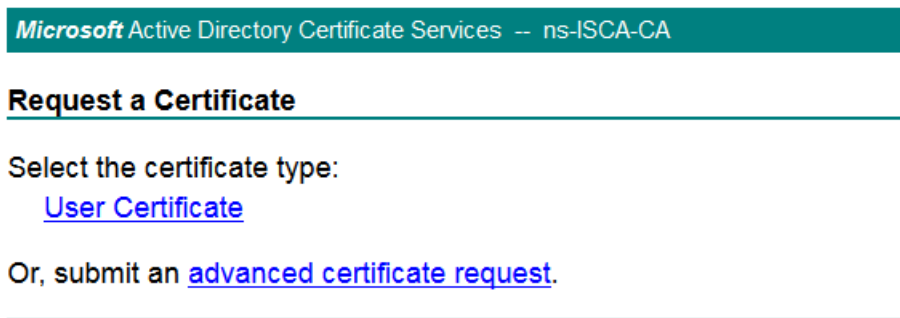
1. Navigate to the **Microsoft Active Directory Certificate Services** page:

Figure 101 *Microsoft Active Directory Certificate Services*



2. Click **Request a certificate**.

Figure 102 *Certificate Services: Request a Certificate*



3. Choose **advanced certificate request**.

The **Submit a Certificate Request or Renewal Request** dialog appears.

This operation submits a saved certificate request to the Certificate Authority.

Figure 103 AD Certificate Services: Submit a Certificate Request

The screenshot shows the 'Submit a Certificate Request or Renewal Request' page in the Microsoft Active Directory Certificate Services console. The page has a teal header with the text 'Microsoft Active Directory Certificate Services -- ns-ISCA-CA' and a 'Home' link. Below the header, the title 'Submit a Certificate Request or Renewal Request' is displayed. A paragraph explains that users should paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request into the 'Saved Request' box. The form includes three main sections: 'Saved Request' with a large text area and a label 'Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):'; 'Certificate Template' with a dropdown menu currently showing 'User'; and 'Additional Attributes' with a smaller text area and a label 'Attributes:'. A 'Submit >' button is located at the bottom of the form.

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 104](#) shows an example of the completed Certificate Request web form.

Figure 104 Completed Submit a Certificate Request Dialog

Microsoft Active Directory Certificate Services -- ns-ISCA-CA [Home](#)

Submit a Certificate Request or Renewal Request

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.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDjCCAFYCAQAwcTEQMA4GA1UEAxMHY3BwbsO1
ZXJpbmcxFTATBgNVBAoTDEFjbWUgU3lzdGVtczEL
BAYTALVTMRYwFAYDVQQHEw1TYW4gRnJhbmNpc2Nv
AAOCAQ8AMIIBCgKCAQEAWReO7c/s2VD3/x1/nV3Q
ebRjnmYzTRciMeFDAD91yheHAIszDGCqQQ7tGPiZ
-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

6. Click **Submit**.
The Certificate Issued dialog appears.


Figure 105 AD Certificate Services: Certificate Issued

Microsoft Active Directory Certificate Services -- ns-ISCA-CA

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

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 W-ClearPass Policy Manager server.

Importing a Server Certificate into W-ClearPass

To import a server certificate into W-ClearPass:

1. Navigate to **Administration > Certificates > Server Certificate**.

The W-ClearPass Policy Manager Server Certificate dialog appears.

Figure 106 W-ClearPass Policy Manager Server Certificate Dialog

Subject:	O=PolicyManager, CN=cppm-5K
Issued by:	O=PolicyManager, CN=cppm-5K
Issue Date:	Oct 09, 2014 16:09:56 PDT
Expiry Date:	Oct 09, 2015 16:09:56 PDT
Validity Status:	Valid
Details:	View Details

2. From the Select Server drop-down menu, select the appropriate W-ClearPass server.
When you select the W-ClearPass Policy Manager server, the *Select Type* field is automatically populated.
3. Select the **Import Server Certificate** link.
The Import Server Certificate dialog is displayed.

Figure 107 Import Server Certificate Dialog

Selected Server:	cppm-5K
Selected Type:	RADIUS Server Certificate
Certificate File:	<input type="button" value="Browse..."/> certnew.cer
Private Key File:	<input type="button" value="Browse..."/> CertPrivKey.pkey
Private Key Password:	●●●●●●

4. Do the following:
 - a. **Certificate File:** Browse to the certificate file that was downloaded by Active Directory Certificate Services.
 - b. **Private Key File:** Browse to the private key file to be imported.
 - c. **Private Key Password:** Specify the private key password that was entered when the Certificate Signing Request was configured.
5. Click **Import**.
The selected server certificate is imported into W-ClearPass. The Server Certificate screen displays the message "Server Certificate updated successfully. Please log in again to continue."

Figure 108 Server Certificate Updated Successfully

ClearPass Policy Manager [Support](#) | [Help](#) | [Logout](#)
admin (Super Administrator)

Administration > Certificates > Server Certificate

Server Certificate

- Create Self-Signed Certificate
- Create Certificate Signing Request
- Import Server Certificate
- Export Server Certificate

Server Certificate updated successfully. Please log in again to continue...

Select Server: Select Type:

Subject:	CN=cppm-5K, OU=Engineering, O=Acme Systems, L=San Francisco, ST=CA, C=US
Issued by:	CN=ns-ISCA-CA, DC=ns, DC=arubatac, DC=us
Issue Date:	Nov 25, 2014 07:31:05 PST
Expiry Date:	May 20, 2015 14:06:49 PDT
Validity Status:	Valid
Details:	View Details

Intermediate CA Certificate:

Subject:	CN=ns-ISCA-CA, DC=ns, DC=arubatac, DC=us
Issued by:	CN=ns-RCA-CA, DC=ns, DC=arubatac, DC=us
Issue Date:	May 20, 2013 13:56:49 PDT
Expiry Date:	May 20, 2015 14:06:49 PDT
Validity Status:	Valid
Details:	View Details

Root CA Certificate:

Subject:	CN=ns-RCA-CA, DC=ns, DC=arubatac, DC=us
Issued by:	CN=ns-RCA-CA, DC=ns, DC=arubatac, DC=us
Issue Date:	May 20, 2013 11:59:22 PDT
Expiry Date:	May 20, 2023 12:09:21 PDT
Validity Status:	Valid
Details:	View Details

6. Log out of the W-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.

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 NTLM authentication (NTLM being the mechanism that W-ClearPass uses to authenticate users) has succeeded.

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 a Dell 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 121](#)).

For authentication purpose, the wireless client can associate with a network access server (NAS) or a RADIUS client. W-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.

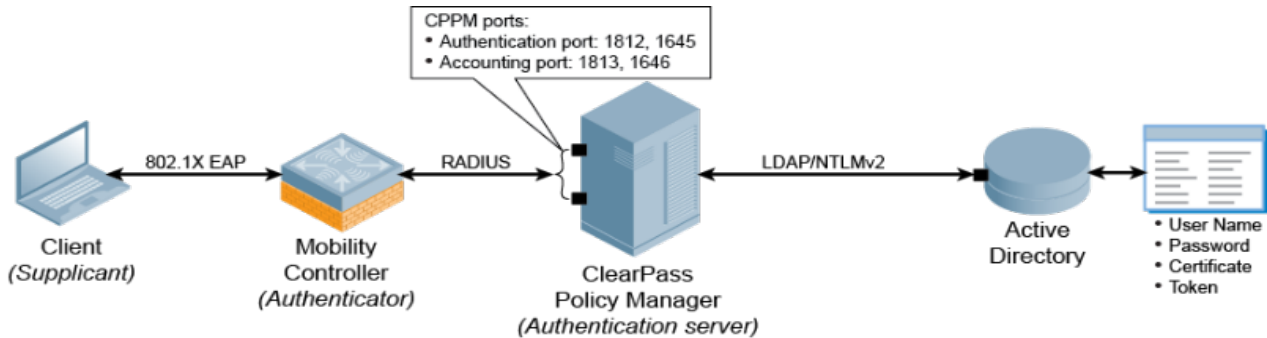
802.1X Authentication Components

802.1x authentication consists of three components—a *supplicant*, an *authenticator*, and an *authentication server* (see [Figure 109](#)).

- 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/W-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 W-ClearPass Policy Manager server.

Figure 109 802.1X Authentication Network Components



[Table 18](#) describes each of the W-ClearPass firewall ports that are used by Active Directory®.

Table 18: Active Directory W-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 (AD DS) 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 Type field. ICMP types echo (8) and echo-reply (0) are used between the CPPM host and the domain controller during the domain join operation (see Joining a W-ClearPass Server to an Active Directory Domain on page 93).

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.

W-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 W-ClearPass Policy Manager as an accounting server, and it is up to the NAS to provide accurate accounting information to W-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 W-ClearPass Policy Manager Service](#)

This section describes how to use the W-ClearPass Policy Manager to configure 802.1X authentication with Active Directory in a Dell 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 93](#)).

The supplicant (wireless client) authenticates against the RADIUS server (which is the authentication server/W-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.)

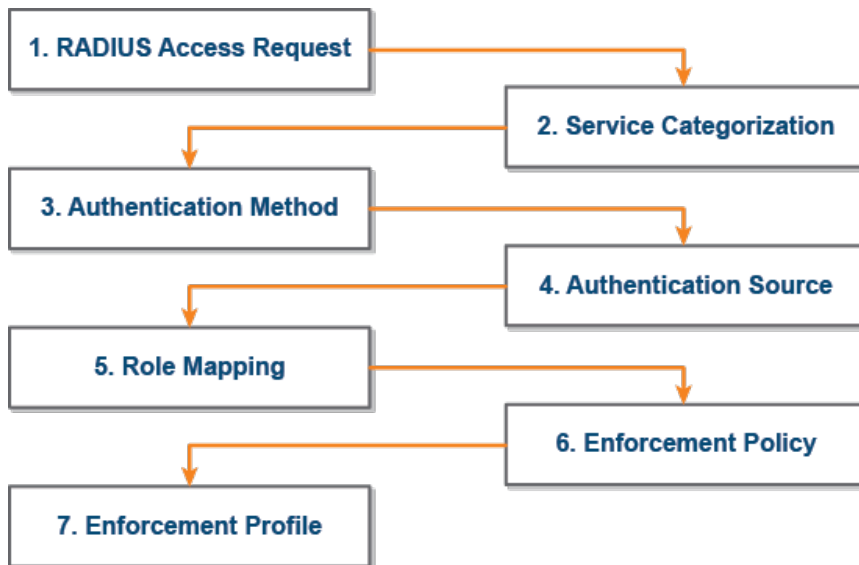
Mobility controllers perform EAP exchanges between the supplicant and convert these to RADIUS access-request messages that are sent to the RADIUS server's IP address and the specified UDP port (for details, see [A Tour of the EAP-PEAP-MSCHAPv2 Ladder on page 191](#)).

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 110](#) illustrates the authentication process flow for an 802.1X Wireless Service.

Figure 110 802.1X Wireless Service Authentication Process Flow



[Table 19](#) provides descriptions of each of the 802.1X authentication processes illustrated in [Figure 110](#).

Table 19: Description of the 802.1X Authentication Processes

	Authentication Process	Description
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 [EAP-PEAP MSCHAPv2 Handshake Exchange Summary on page 191](#).

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.

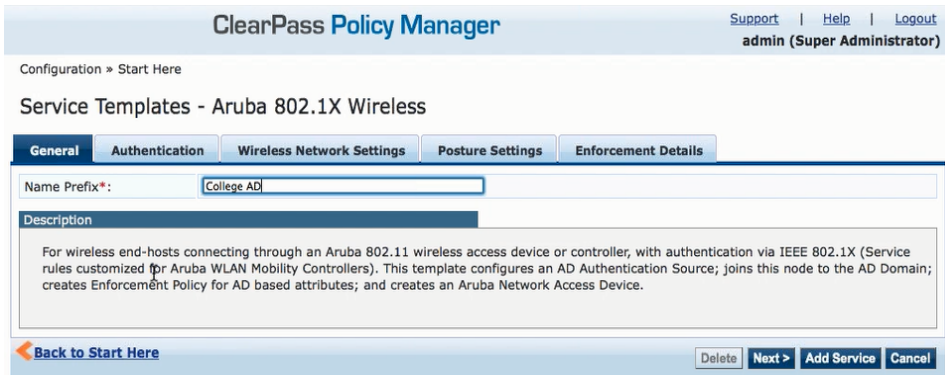
This W-ClearPass 802.1X template guides you through the following tasks:

- 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](#).
- 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 W-ClearPass Policy Manager Integration](#).
- Creating an Enforcement Policy for Active Directory-based attributes.
The procedure for creating an Enforcement Policy is described in this section.

To create the 802.1X wireless service:

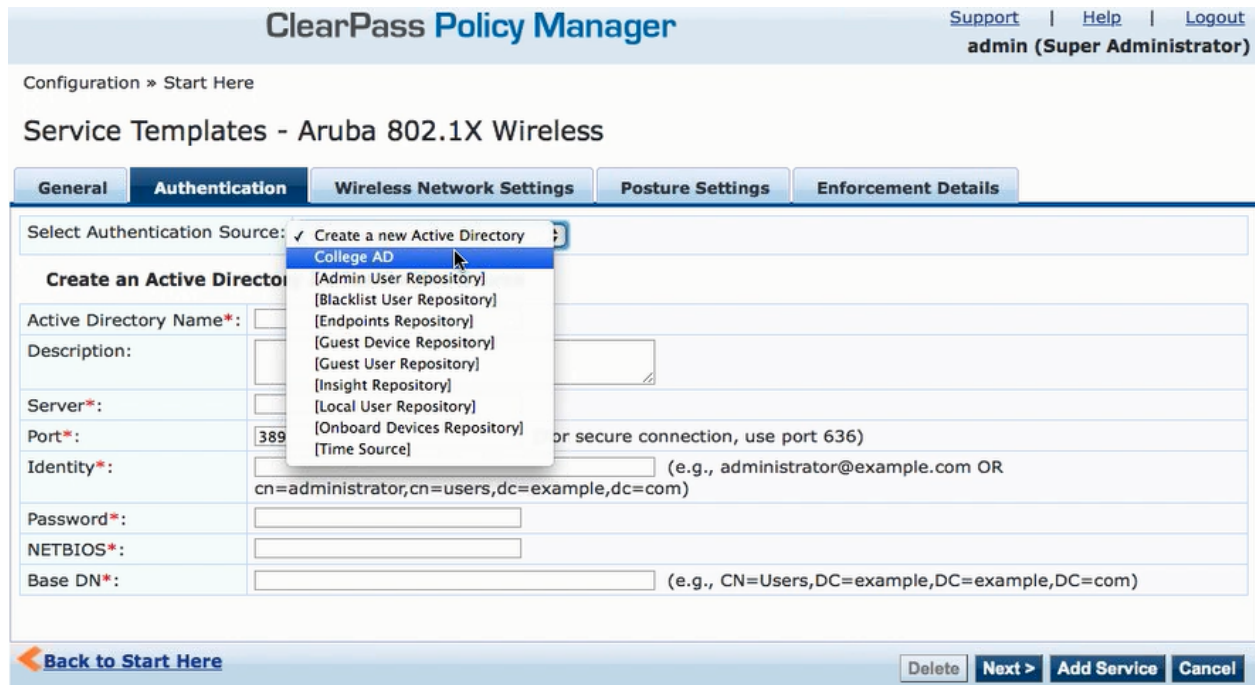
1. From W-ClearPass Policy Manager, navigate to **Configuration > Start Here > Aruba 802.1x Wireless**. The **General** page for the W-ClearPass 802.1X Wireless Service template opens.

Figure 111 General Page in the 802.1X Wireless Service Template



2. In the *Name Prefix* field, enter a prefix that is appended to services using this template, then click **Next**. The **Authentication** page is displayed.
3. From the **Select Authentication Source** drop-down list, select the name of the Active Directory, as shown in [Figure 112](#), then click **Next**.

Figure 112 Selecting the Active Directory



When you choose an existing Authentication Source, the information in the **Authentication** and **Enforcement Details** pages is populated automatically.

The Wireless Network Settings page appears.

4. Select the mobility controller you defined earlier (for details, see [Preparing the Mobility Controller for W-ClearPass Policy Manager Integration](#)).

Figure 113 *Selecting the Mobility Controller*

The screenshot shows the ClearPass Policy Manager interface. At the top, it says "ClearPass Policy Manager" and "admin (Super Administrator)". Below that, it says "Configuration » Start Here". The main heading is "Service Templates - Aruba 802.1X Wireless". There are five tabs: "General", "Authentication", "Wireless Network Settings" (which is selected), "Posture Settings", and "Enforcement Details". The "Wireless Network Settings" tab contains the following fields:

Select wireless controller:	Aruba3400
Wireless Controller Name:	Aruba3400
Controller IP Address:	10.162.114.2
Vendor Name:	Aruba
RADIUS Shared Secret:	*****
Enable RADIUS CoA:	<input checked="" type="checkbox"/>
RADIUS CoA Port:	3799

At the bottom of the form, there are buttons: "Back to Start Here", "Delete", "Next >", "Add Service", and "Cancel".

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 appears.

Figure 114 *Enabling Posture Checks*

The screenshot shows the ClearPass Policy Manager interface. At the top, it says "ClearPass Policy Manager" and "admin (Super Administrator)". Below that, it says "Configuration » Start Here". The main heading is "Service Templates - Aruba 802.1X Wireless". There are five tabs: "General", "Authentication", "Wireless Network Settings", "Posture Settings" (which is selected), and "Enforcement Details". The "Posture Settings" tab contains the following field:

Enable Posture Checks:	<input checked="" type="checkbox"/>
------------------------	-------------------------------------

At the bottom of the form, there are buttons: "Back to Start Here", "Delete", "Next >", "Add Service", and "Cancel".

W-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 appears.

[Figure 115](#) 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 115 *Creating a New Enforcement Policy*

Table 20: *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"> Configure an optional enforcement policy based on the following attributes: <ul style="list-style-type: none"> Department Email Name Phone Title UserDN company member of
Attribute Value	<ol style="list-style-type: none"> Enter the Active Directory attribute value for the selected name in the <i>Attribute Name</i> field.
Aruba Role	<ol style="list-style-type: none"> Assign a user role to the Enforcement Policy. The configured user roles are defined in the mobility controller specified for this service. To see the list of configured user roles defined in the mobility controller: <ol style="list-style-type: none"> Log in to the Mobility Controller. Navigate to Configuration > SECURITY > Access Control. The User Roles page is displayed.

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 116 Summary of the 802.1X Service Configuration

Configuration » Services

Services

- Added 5 Enforcement Profile(s)
- Added 1 Enforcement Policies
- Added 1 service(s)

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

#	Order	Name	Type	Template	Status
1.	1	[Policy Manager Admin Network Login Service]	TACACS	TACACS+ Enforcement	●
2.	2	[AirGroup Authorization Service]	RADIUS	RADIUS Enforcement (Generic)	●
3.	3	[Aruba Device Access Service]	TACACS	TACACS+ Enforcement	●
4.	4	[Guest Operator Logins]	Application	Aruba Application Authentication	●
5.	5	College AD Aruba 802.1X Wireless	RADIUS	Aruba 802.1X Wireless	●

Showing 1-5 of 5 Reorder Copy Export Delete

Deleting a W-ClearPass Policy Manager Service

You can only delete W-ClearPass services that have been created by an administrator. Default services cannot be deleted.

To delete a W-ClearPass Policy Manager service:

1. Navigate to **Configuration > Services**.
The **Configuration > Services** page opens.

Figure 117 Deleting a W-ClearPass Service

ClearPass Policy Manager Support | Help | Logout admin (Super Administrator)

Configuration » Services

Services

- Add
- Import
- Export All

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

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

Showing 1-4 of 4 Reorder Copy Export Delete

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.

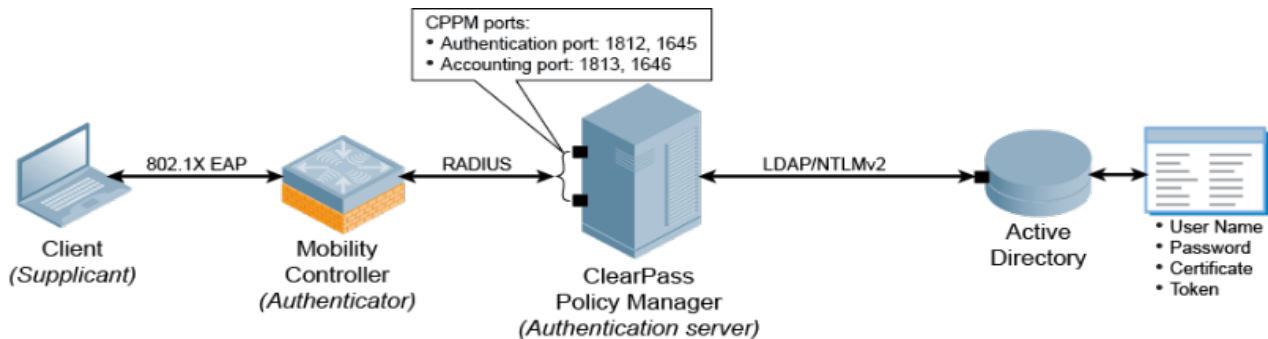
Walking Through an 802.1X Authentication Scenario

This section shows the flow 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 118](#) shows the flow of traffic for 802.1X authentication using Active Directory.

Figure 118 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 118](#).

1. A Sales Department employee connects to the Dell wireless network from his 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.
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 W-ClearPass Policy Manager server with the encrypted username and password.
RADIUS is the protocol that network access device (NAD) authenticators use to communicate with the W-ClearPass server in order to look up the information in the RADIUS database, which in this example is Active Directory.
4. The W-ClearPass Policy Manager server checks the Active Directory database for a matching username and password.
The communication between the W-ClearPass Policy Manager server and Active Directory is via NTLM (NT LAN Manager) for authentication in conjunction with LDAP (Lightweight Directory Access Protocol) for search and directory lookup.
 - If there is not a match, the W-ClearPass Policy Manager server sends an *access-reject* message to the mobility controller.
 - If there is a match, the W-ClearPass Policy Manager server sends an *access-accept* message to the mobility controller, and the user is granted access to the network.

User Role Attribute Information

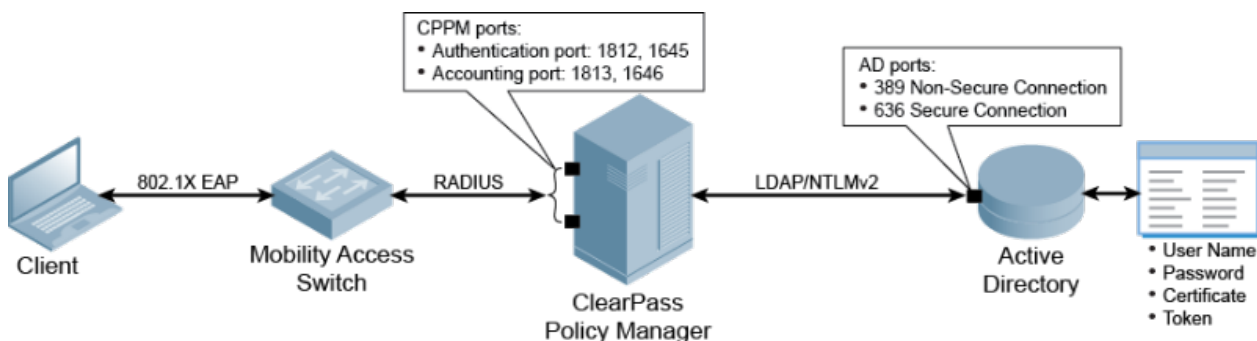
The W-ClearPass Policy Manager server can also send attribute information about the user (for example, User Role) to the mobility controller. In this example, the server uses the User Role attribute, which indicates that the user is in the Sales Department.

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 a Mobility Access Switch (MAS) or a third-party switch and perform 802.1X authentication to the W-ClearPass Policy Manager server (see [Figure 119](#)).

Figure 119 Traffic flow for 802.1X Wired Authentication with Active Directory



For more information about the Dell Mobility Access Switch and 802.1X authentication, see [Mobility Access Switch Configuration for 802.1X Authentication on page 165](#).

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 hostname instead of an IP address for Active Directory server in the **Server** field (see), ensure that the Active Directory hostname is resolved 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 username used for Bind DN is not locked in the Active Directory.
4. While joining W-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 W-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 the Date and Time Are in Sync on page 94](#)).



The maximum allowed clock skew between the W-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, verify the following:
 - a. Verify the shared secret in the mobility controller and W-ClearPass Policy Manager's Network Access Device configuration. Shared secret errors are shown in the W-ClearPass Policy Manager Event Viewer.
 - b. Ensure that the mobility controller's IP address is configured correctly in W-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 includes the following information:

- [W-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 W-ClearPass Insight in a Cluster](#)
- [Configuring Cluster File-Backup Servers](#)
- [Using High Capacity Guest Mode](#)
- [Cluster CLI Commands](#)

W-ClearPass Cluster Overview

This section contains the following information:

- [Introduction](#)
- [W-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 W-ClearPass hardware or virtual appliances.

This chapter provides guidance on how to design and deploy W-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 and enable and use High Capacity Guest Mode. Finally, the set of cluster-specific CLI commands is included.

W-ClearPass Policy Manager can be deployed either as a dedicated hardware appliance or a virtual machine running on top of VMware ESX/ESXi or Microsoft Hyper-V. W-ClearPass supports a 500, 5,000, or a 25,000 endpoints hardware or virtual appliance. For more information on the Dell hardware and virtual appliances, refer to [About W-ClearPass on page 11](#).

When you deploy W-ClearPass in High Guest Capacity mode, the node can support 1,000, 10,000 and 50,000 guests per day. For more information, see [Using High Capacity Guest Mode on page 157](#).

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 W-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 W-ClearPass Insight in a Cluster on page 152](#)).

W-ClearPass Databases

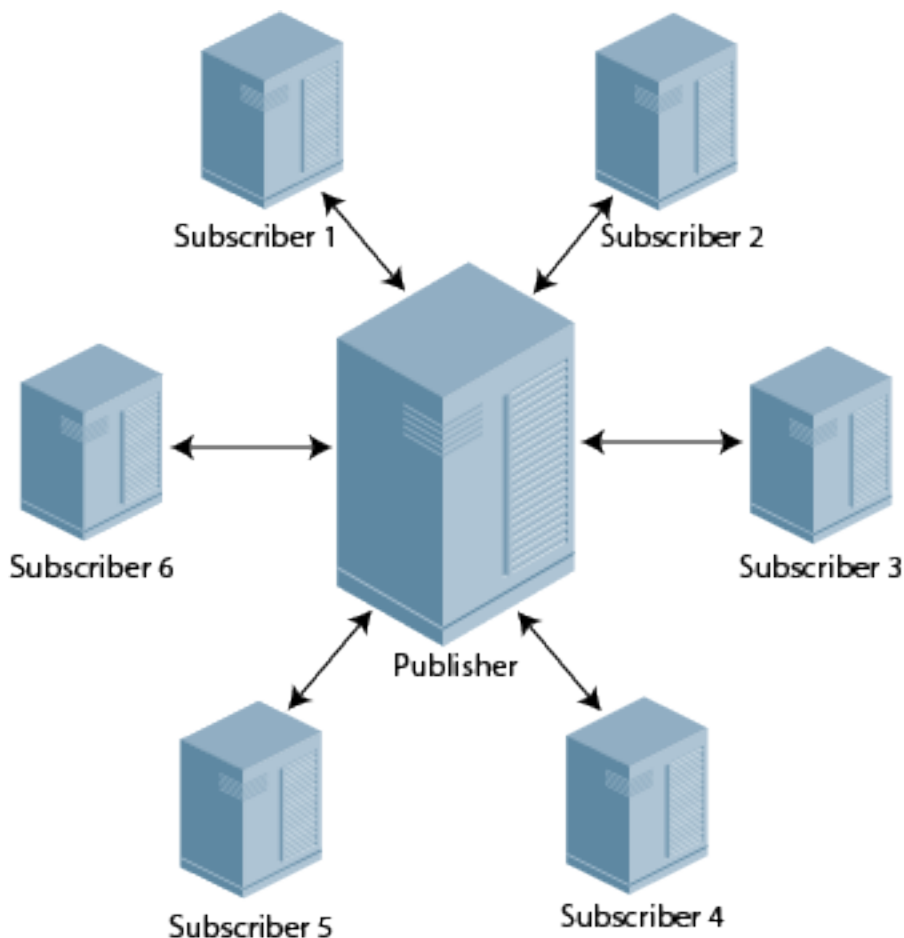
Each W-ClearPass server makes use of the following databases:

- **Configuration database.** Contains most of the editable entries that can be seen in the W-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 W-ClearPass Insight in a Cluster on page 152](#)).

Publisher/Subscriber Model

W-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 120 *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.
- 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 CPPM 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 21](#) lists the network ports that must be opened between the Publisher and the Subscriber nodes.

Table 21: *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 21](#) 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 W-ClearPass components scale differently (see [Table 22](#)).

Table 22: *W-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](#)
- [RTT Considerations When Building Geographically Distributed Clusters](#)
- [Implementing W-ClearPass Zones for Geographical Regions](#)

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

Cluster Deployment Sizing Guidance

The maximum single cluster size is limited to 30 nodes.

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

To determine the optimum sizing for a W-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 W-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 W-ClearPass hardware appliances you would need, with redundancy ranging from (N+1) to full redundancy, depending on the needs of the customer.

EAP-TLS Performance

EAP-TLS raw performance on a W-ClearPass 25K class hardware appliance without any authorization source configured can be as high as 300 authentications per second, with an average latency of around 300 ms (with the CPU running at 50%).

EAP-PEAP-MSCHAPv2 Performance

EAP-PEAP-MSCHAPv2 raw performance on a W-ClearPass 25K class hardware, with Active Directory-based authentication and authorization, can be as high as 400 authentications per second, with an average latency of around 300 ms (with the CPU running at 50%).

Publisher Node Guidelines

Setting Up a Standby Publisher

W-ClearPassPolicy 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 144](#).

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 W-ClearPass Insight database. However, take care to carefully monitor the Publisher node's capacity and performance.
- [Table 23](#) shows the recommended Publisher node disposition that should be deployed given the number and type of Subscribers in the cluster.

Table 23: *Subscriber and Publisher Deployment Matrix*

Subscriber Nodes	Publisher Disposition
CP-HW-500 Subscriber Nodes	
4 or less CP-HW-500 Subscriber nodes	Dedicated CP-HW-500 Publisher pair
5 to 20 CP-HW-500 Subscriber nodes NOTE: Assumes less than 4,000 unique endpoints.	Dedicated CP-HW-5K Publisher pair
21+ CP-HW-500 Subscriber nodes	Dedicated CP-HW-25K Publisher pair
CP-HW-5K Subscriber Nodes	
4 or fewer CP-HW-5K Subscriber nodes	Dedicated CP-HW-5K Publisher pair
5+ CP-HW-5K Subscriber nodes	Dedicated CP-HW-25K Publisher pair
CP-HW-25K Subscriber Nodes	
Up to 10 CP-HW-25K Subscriber nodes	Dedicated CP-HW-25K Publisher pair

Subscriber Node Guidelines

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, 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 used, ensure that the EAP-TLS authentication method in Policy Manager is configured to perform *localhost* OCSP checks.

Providing Sufficient Bandwidth Between Publisher and Subscribers

In a large-scale deployment, reduced bandwidth or high latency on the link (greater than 200ms) 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
Not a significant consumer of bandwidth.
- 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 100KB.
- Guest/Onboard configuration changes
Only the changes to the database configuration are sent, and this information is typically small in size (approximately 10KB).

RTT Considerations When Building Geographically Distributed Clusters

It's important to take the delay between a W-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.

- Dell recommends that the round-trip time between the NAD/NAS and a W-ClearPass server should not exceed 600ms.
- The acceptable delay between cluster nodes is less than 50ms (RTT less than 100ms).

- The link bandwidth should be greater than 10Mbps.

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 W-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 W-ClearPass Zones for Geographical Regions

W-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 as well as between all the Subscribers in the cluster.

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

W-ClearPass uses 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'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 W-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.

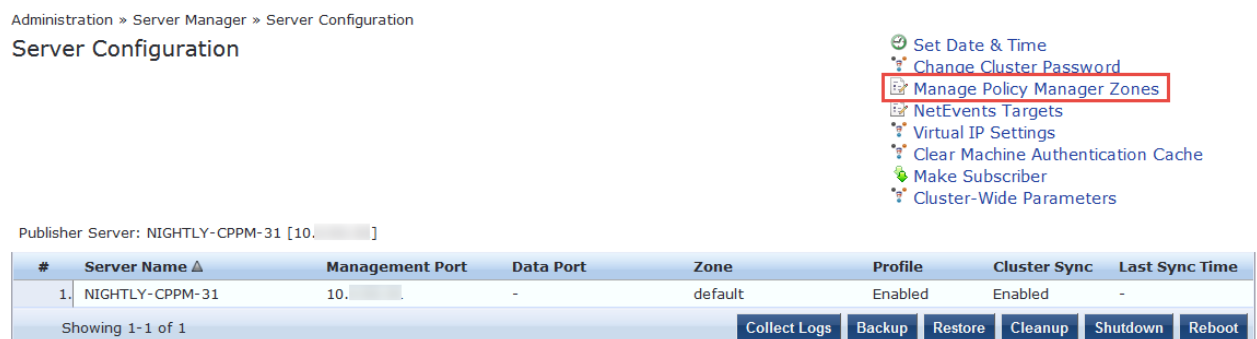
Creating Geographical Zones in Policy Manager

You can configure zones in W-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 W-ClearPass Policy Manager nodes that share their runtime state.

To create geographical zones in Policy Manager:

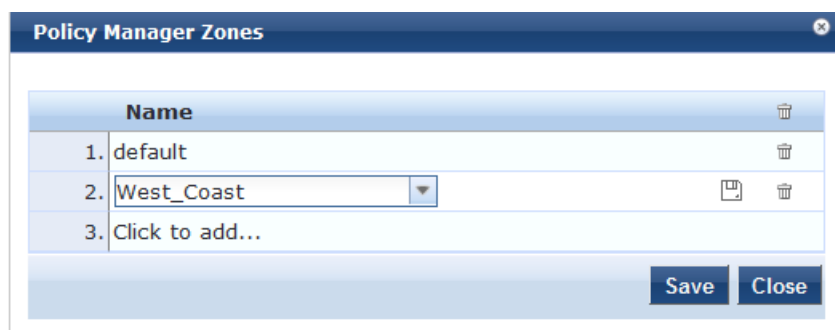
1. Navigate to the **Administration > Server Manager > Server Configuration** page.

Figure 121 Manage Policy Manager Zones Link



2. Click the **Manage Policy Manager Zones** link.
The Policy Manager Zones dialog appears.
3. Select **Click to add...**
A blank field appears in the dialog.

Figure 122 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 Dell 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 W-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 W-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 Subscribers 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. CPPM clustering can also be performed for other reasons, for example, to distribute several CPPM nodes geographically for policy reasons, or to have an off-site disaster recovery system.

Design Guidelines

- The dedicated Publisher should be a W-ClearPass 25K hardware appliance (CP-HW-25K) or a W-ClearPass 25K Virtual Appliance (CP-VM-25K) that matches the minimum specification for the CP-VM-25K virtual appliance:

Table 24: W-ClearPass 25K 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 NOTE: For a 40-60 read/write profile for 4K random read/write

- 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 PPolicy Manager post-authentication profile.

Examples of Customer Cluster Deployments

This section provides two examples of typical customer cluster deployments.

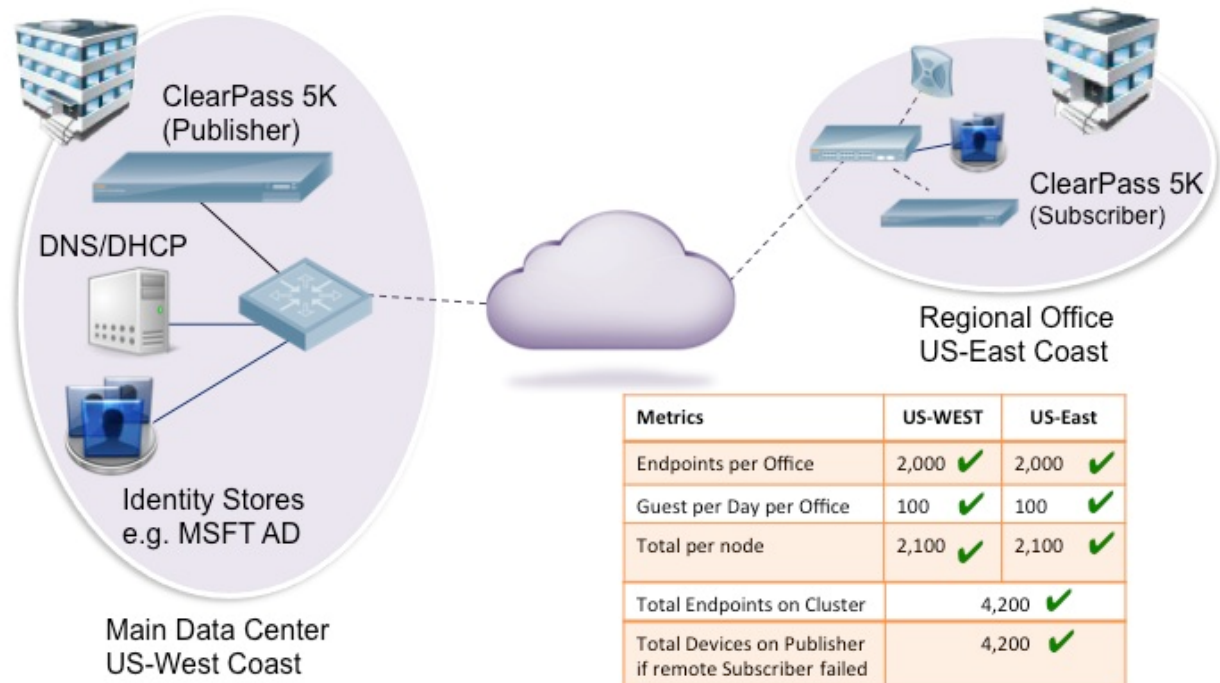
Authenticating Corporate Users with Guest Access

In this example, a cluster of W-ClearPass 5K hardware appliances (CP-HW-5K) has two nodes—U.S. East Coast and U.S. West Coast (see [Figure 123](#)).

- *US-West* is the Publisher.
- *US-East* is the Subscriber.
- 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 123 Example of a Medium-Scale Cluster Deployment



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

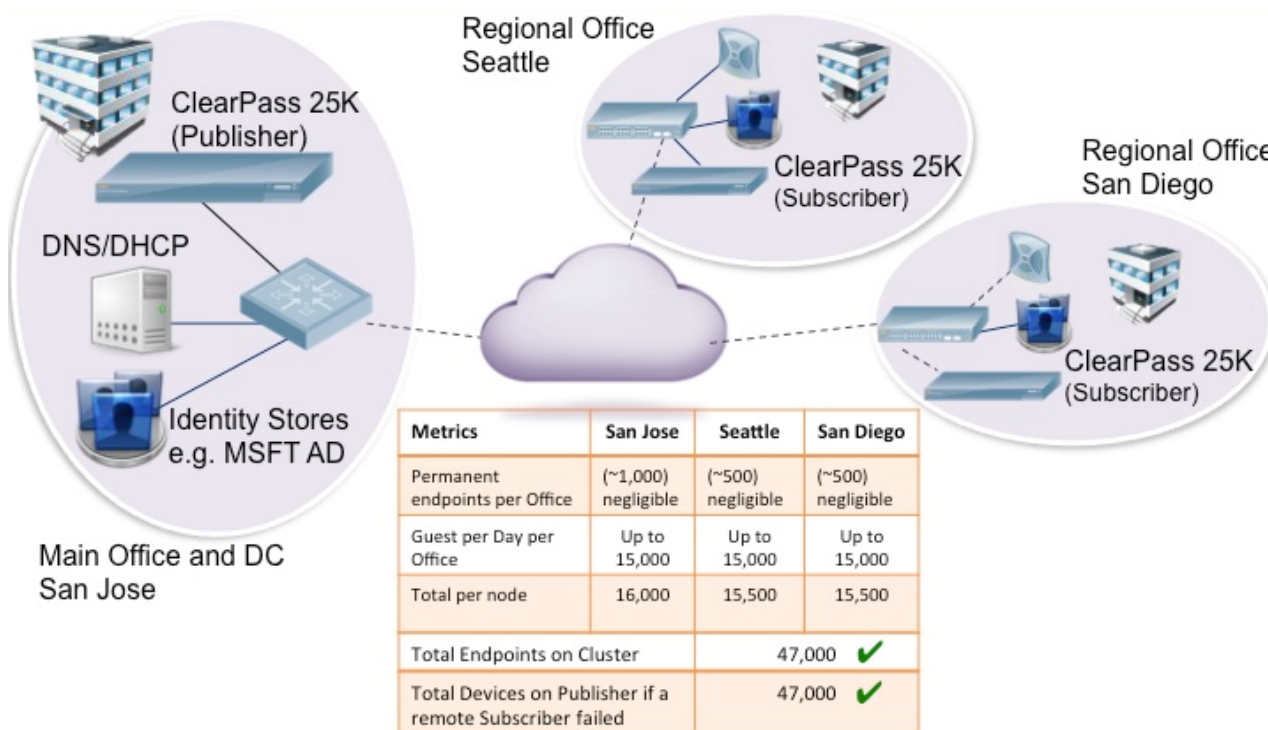
- The additional load on the Publisher due to clustering can be estimated at 100 guest accounts created per day.
- The authentication traffic on the Subscriber node does not impose any additional load on the Publisher and the new endpoints registered (in the order of 100 per day, assuming new guests 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 W-ClearPass 25K hardware appliance nodes (CP-HW-25) in the same time-zone (see [Figure 124](#)).

- 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 124 Example of a Large-Scale Cluster Deployment



The cluster illustrated in [Figure 124](#) 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 W-ClearPass 25K hardware appliance (CP-HW-25K).

The W-ClearPass 25K 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

W-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 W-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 125 *Standby Publisher Dialog*

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

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

Table 25: *Configuring Standby Publisher Parameters*

Parameter	Action/Description
Enable Publisher Failover	1. To authorize a node in a cluster on the system to act as a Publisher if the primary Publisher fails, select TRUE . The default value is FALSE .
Designated Standby Publisher	2. From the drop-down, select the CPPM server in the cluster that will serve as the Standby Publisher.
Failover Wait Time	3. 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.
	4. When finished, click Save .

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.

The process used to verify the reachability of the remote W-ClearPassPolicy Manager nodes uses an outbound HTTPS call. As noted in [Network Ports That Must Be Enabled on page 134](#), 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](#)).



It is good practice that 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 W-ClearPass Policy Manager functions are temporarily lost:

- AirGroup and MACTrac enrollment
- Certificate creation and revocation
- Certificate revocation list updates
- W-ClearPass Exchange outbound enforcement
- General W-ClearPass Policy Manager and W-ClearPass Guest configuration changes
- W-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

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

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

Figure 126 *Server Configuration > Make Subscriber Option*

Administration » Server Manager » Server Configuration

Server Configuration

- Set Date & Time
- Change Cluster Password
- Manage Policy Manager Zones
- NetEvents Targets
- Virtual IP Settings
- Clear Machine Authentication Cache
- Make Subscriber**
- Upload Nessus Plugins
- Cluster-Wide Parameters

Publisher Server: VM-103 [10.17.6.103]

#	Server Name ▲	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	VM-103	10.17.6.103	-	default	Enabled	Enabled	-

Showing 1-1 of 1

Collect Logs Backup Restore Cleanup Shutdown Reboot

3. Click **Make Subscriber**.
The **Add Subscriber Node** dialog opens.

Figure 127 *Configuring the Subscriber Node*

Add Subscriber Node

Publisher IP: 10.10.5.5

Publisher Password: ●●●●●●

Restore the local log database after this operation

Do not back up the existing databases before this operation

WARNING :

- 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.

Save Cancel

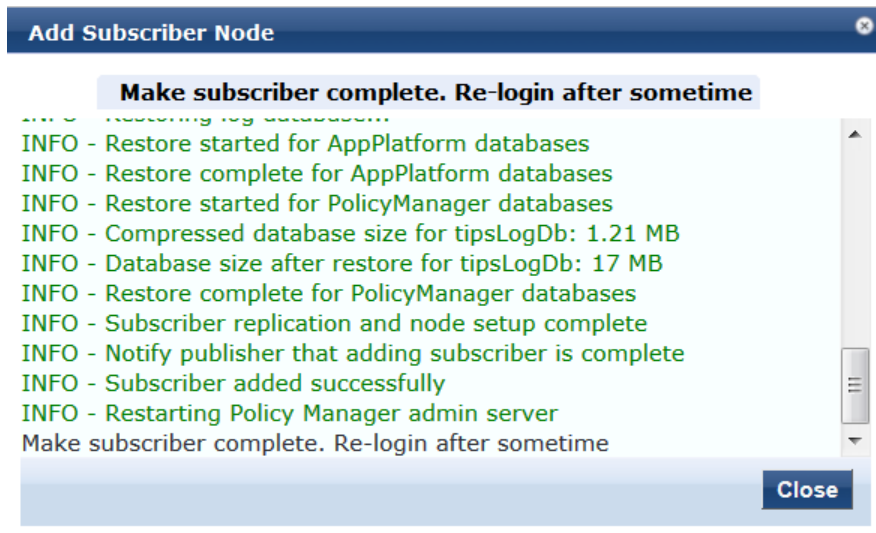
4. Specify the **Add Subscriber Node** parameters as described in [Table 26](#).

Table 26: *Configuring Add Subscriber Node Parameters*

Parameter	Action/Description
Publisher IP	1. Enter the Publisher node's IP address.
Publisher Password	2. Enter the appadmin (CLI) password.
Restore the local log database after this operation	3. To restore the log database following the addition of a Subscriber node, select the check box.
Do not backup the existing databases before this operation	4. Select this check box only if you do not require a backup to the existing database.

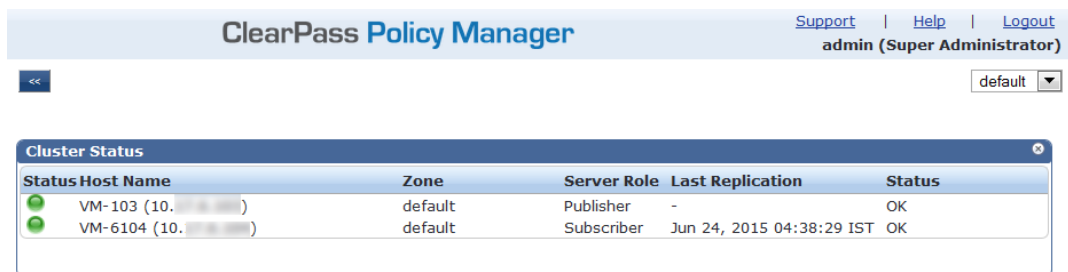
- Be sure to note the warnings on this dialog and respond as needed.
- When finished, click **Save**.
You will see the message: *Adding node as subscriber to <IP_address>'s cluster.*
When the process completes, the following messages are displayed:

Figure 128 *Completing Subscriber Setup*



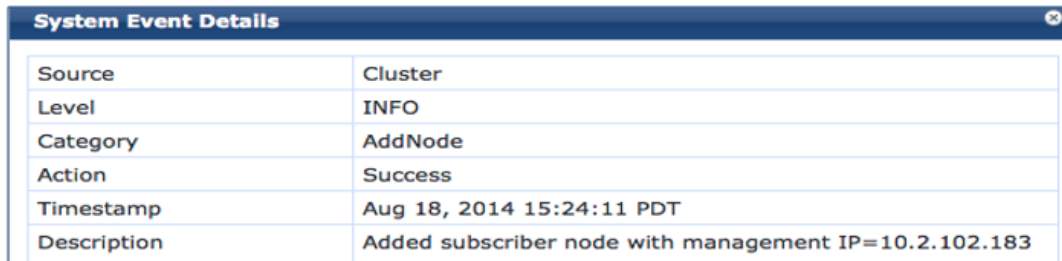
- To complete the Subscriber setup, log back into the new Subscriber node.
When you log into the Publisher node or the Subscriber node, the Policy Manager Dashboard presents the updated cluster status:

Figure 129 *Cluster Status: Subscriber Node Added*



You can also track this process in the Event Viewer following a successful Subscriber addition, as shown in [Figure 130](#).

Figure 130 Tracking the Add Node Process in the Event Viewer



System Event Details	
Source	Cluster
Level	INFO
Category	AddNode
Action	Success
Timestamp	Aug 18, 2014 15:24:11 PDT
Description	Added subscriber node with management IP=10.2.102.183

Using the CLI to Create a Subscriber Node

You can make a node a Subscriber via the command line interface.

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

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

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

```
cluster make-subscriber -I [publisher IP address]
```

Figure 131 Description of the **cluster make-subscriber** command

```
[appadmin@cppm183.cppm-testing.com]# cluster make-subscriber
Usage:
make-subscriber -i <IP Address> [-l] [-b]

-i <IP Address> -- Publisher IP Address
-l              -- Restore the local log database after this operation
-b             -- skip generating a backup before this operation
```

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

Figure 132 Subscriber 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 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 133 *Selecting the Subscriber Node to Remove*

Administration > Server Manager > Server Configuration

Server Configuration

- Set Date & Time
- Change Cluster Password
- Manage Policy Manager Zones
- NetEvents Targets
- Virtual IP Settings
- Clear Machine Authentication Cache
- Upload Nessus Plugins
- Cluster-Wide Parameters

Publisher Server: p.india.avendasys.com [10.17.4.69]

#	Server Name ▲	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
21.	Sub1-V8-500.india.avendasys.com	10. [redacted]	-	default	Enabled	Disabled	-
22.	Sub2-V8-500.india.avendasys.com	10. [redacted]	-	default	Enabled	Disabled	-

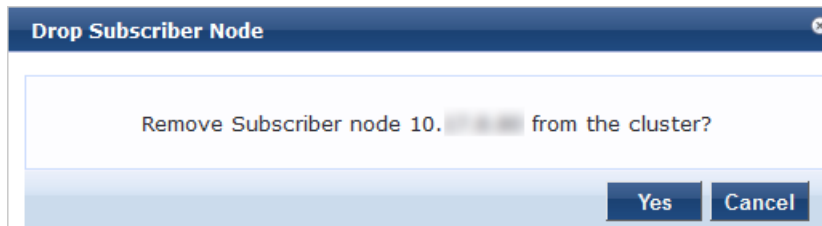
Showing 21-22 of 22

Collect Logs Backup Restore Cleanup Shutdown Reboot **Drop Subscriber**

3. Click **Drop Subscriber**.

You are prompted to confirm the drop action.

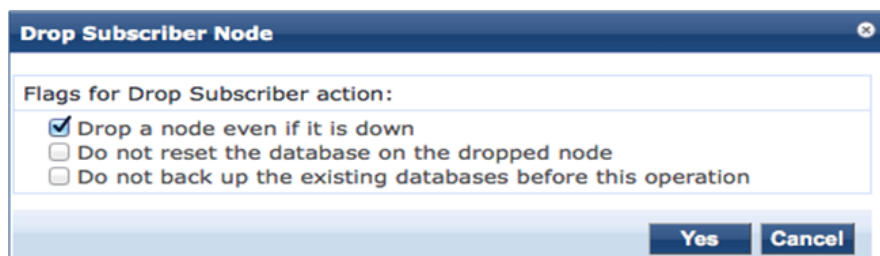
Figure 134 *Confirming the Drop Subscriber Operation*



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 135 Drop Subscriber Node Confirmation Options



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

- Drop a node even if it's 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 subscriber node is removed from the cluster.

Rejoining a Node Back Into the Cluster

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

To rejoin a disabled node back into the cluster:

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

[Figure 136](#) shows that one of the subscribers in the cluster is disabled.

Figure 136 Server Configuration Page Showing Disabled Cluster Node

Administration » Server Manager » Server Configuration

Server Configuration

- Set Date & Time
- Change Cluster Password
- Manage Policy Manager Zones
- NetEvents Targets
- Virtual IP Settings
- Clear Machine Authentication Cache
- Cluster-Wide Parameters

Publisher Server: vm-69 [10.10.10.10]

#	Server Name ▲	Management Port	Data Port	Zone	Profile	Cluster Sync	Last Sync Time
1.	vm-65	10.10.10.10	-	default	Enabled	Disabled	Jan 16, 2015 14:08:28 IST
2.	vm-66	10.10.10.10	-	default	Enabled	Enabled	Jan 16, 2015 14:26:29 IST
3.	vm-69	10.10.10.10	-	default	Enabled	Enabled	-

Showing 1-3 of 3

Collect Logs Backup Restore Cleanup Shutdown Reboot Drop Subscriber

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

The **Server Configuration > System** dialog appears for the selected node. As shown in [Figure 137](#), the dialog includes the **Join server back to cluster** option.

Figure 137 Join Server Back to Cluster Option Displayed

Administration » Server Manager » Server Configuration - vm-69
Server Configuration - vm-69 (10.)

- Set Time Zone
- Synchronize Cluster Password
- Promote To Publisher
- Join server back to cluster

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	vm-69				
FQDN:					
Policy Manager Zone:	default				Manage Policy Manager Zones
Enable Profile:	<input checked="" type="checkbox"/> Enable this server for endpoint classification				
Enable Performance Monitoring Display:	<input type="checkbox"/> Enable this server for performance monitoring display				
Insight Setting:	<input type="checkbox"/> Enable Insight				
Span Port:	-- None --				

3. Click **Join server back to cluster**.

A warning message appears, providing the option to promote the current node to publisher status:

Figure 138 Option to Promote Disabled Node to Publisher

Join server back to cluster

Join server 10. back to cluster?

Promote to Publisher?

WARNING : All data that is not synced from the failed publisher will be lost (like new guest accounts that does not exist in current running publisher).

Yes Cancel

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 W-ClearPass Insight in a Cluster

This section contains the following information:

- [Introduction](#)
- [W-ClearPass Insight Placement Considerations](#)
- [When a W-ClearPass Insight-Enabled Node Is Down](#)
- [Enabling W-ClearPass Insight](#)

Introduction

Multiple functions are dependent on W-ClearPass Insight for them to function, for example, MAC caching. W-ClearPass Insight must be enabled on at least one node within a cluster.



Enabling W-ClearPass Insight on at least two nodes in the cluster is recommended.

As you enable W-ClearPass Insight on additional nodes in the cluster, CPPM automatically adds these nodes to the W-ClearPass Insight database authentication source definition.

W-ClearPass Insight does not replicate data to any other nodes within the cluster—it is an entirely stand-alone database.

W-ClearPass Insight Placement Considerations

Having W-ClearPass Insight enabled on multiple nodes within the cluster provides for a level of resilience, however, you need to carefully consider where you enable W-ClearPass Insight. For every node where W-ClearPass Insight is enabled, all the other nodes within the cluster subscribe through *NetEvents* to send data to the W-ClearPass Insight database.

The amount of data sent to the W-ClearPass Insight database can be extremely high, and if you use Insight for processing authentication requests within your cluster, where you enable W-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 W-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 W-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, W-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.
- W-ClearPass Insight data is valuable and could be used as part of policy evaluation. If this is the case, Dell recommends that you enable redundant W-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, W-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 W-ClearPass Insight database. However, take care to carefully monitor the publisher node's capacity and performance.

When a W-ClearPass Insight-Enabled Node Is Down

When a W-ClearPass Insight-enabled node in a cluster is down or out-of-sync for more than 30 minutes, the W-ClearPass Insight node is moved to be the last W-ClearPass Insight node in the fall-back list. This allows for fail-through to other W-ClearPass Insight nodes.

When a W-ClearPass Insight-enabled node is dropped from the cluster, the corresponding node entry in the W-ClearPass Insight repository is removed.

Enabling W-ClearPass Insight

W-ClearPass Insight is not enabled by default, so you must manually enable it.

To enable W-ClearPass Insight:

1. Navigate to **Administration > Server Manager > Server Configuration**.
2. From the **Server Configuration** page, select the W-ClearPass node you want to configure.
The **Server Configuration** dialog opens.

System	Services Control	Service Parameters	System Monitoring	Network	FIPS
Hostname:	NIGHTLY-CPPM-31				
FQDN:					
Policy Manager Zone:	default				Manage Policy Manager Zones
Enable Profile:	<input checked="" type="checkbox"/> Enable this server for endpoint classification				
Enable Performance Monitoring Display:	<input checked="" type="checkbox"/> Enable this server for performance monitoring display				
Insight Setting:	<input checked="" type="checkbox"/> Enable Insight		<input checked="" type="checkbox"/> Enable as Insight Master		Current Master:-
Enable Ingress Events Processing:	<input type="checkbox"/> Enable Ingress Events processing on this server				
Span Port:	-- None --				

- To enable the W-ClearPass Insight reporting tool on this node, select the **Enable Insight** check box.
 - When you enable this check box on a cluster node, the W-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 W-ClearPass Insight Repository is the same order in which W-ClearPass Insight was enabled on those servers.
- 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 W-ClearPass Insight enabled.
- When finished with enabling W-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:

W-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:

- Navigate to the **Administration > External Servers > File Backup Servers** page. The **File Backup Server** page opens.
- Click the **Add** link (at the top-right). The **Add File Backup Server** page opens.

Figure 139 Add File Backup Servers Page

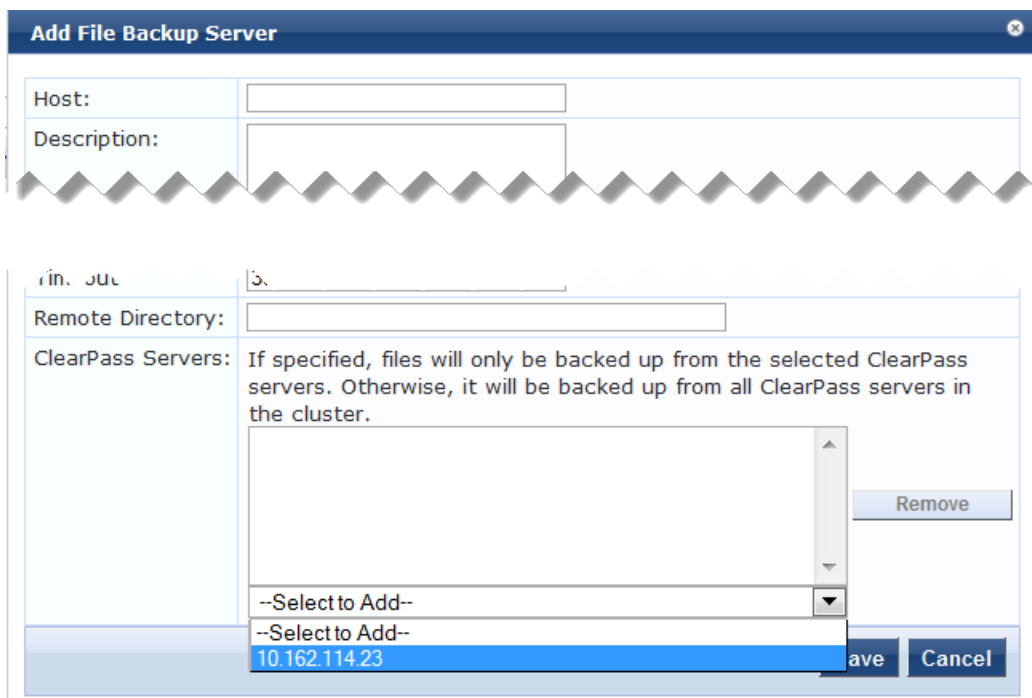
Table describes the **Add File Backup Server** page parameters.

Table 27: Add File Backup Page Server Page Parameters

Parameter	Action/Description
Host	1. Enter the name or IP address of the host.
Description	2. Enter the description that provides additional information about the File Backup server.
Protocol	3. Specify the protocol to be used to upload the generated reports to an external server. Select from the following protocols: <ul style="list-style-type: none"> • SFTP (SSH File Transfer Protocol) • SCP (Session Control Protocol)
Port	4. Specify the port number. The default port is 22 .
Username	5. Enter the user name and password of the host server, then verify the password.
Password	

Parameter	Action/Description
Timeout	6. Specify the timeout value in seconds. The default value is 30 seconds.
Remote Directory	7. 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 W-ClearPass servers in the W-ClearPass Servers field.
ClearPass Servers	8. From the Select to Add drop-down, select the cluster-file backup server(s) to be backed up. When you select specific W-ClearPass servers, files are backed up from the selected W-ClearPass servers only. Otherwise, the files from all the W-ClearPass servers in the cluster are backed up.

Figure 140 Specifying the File Backup Server



9. When finished, click **Save**.

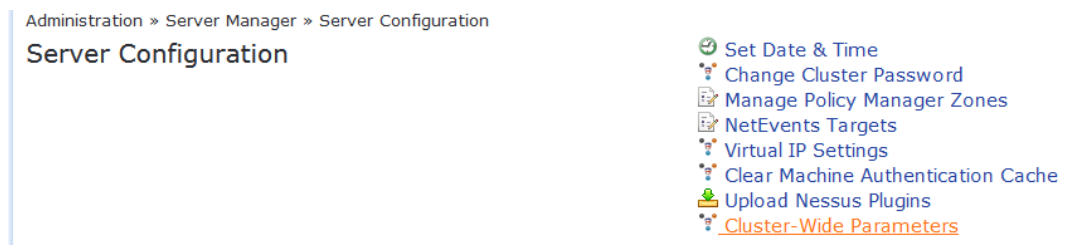
Backing Up Configuration and Access Tracker Log Information

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:

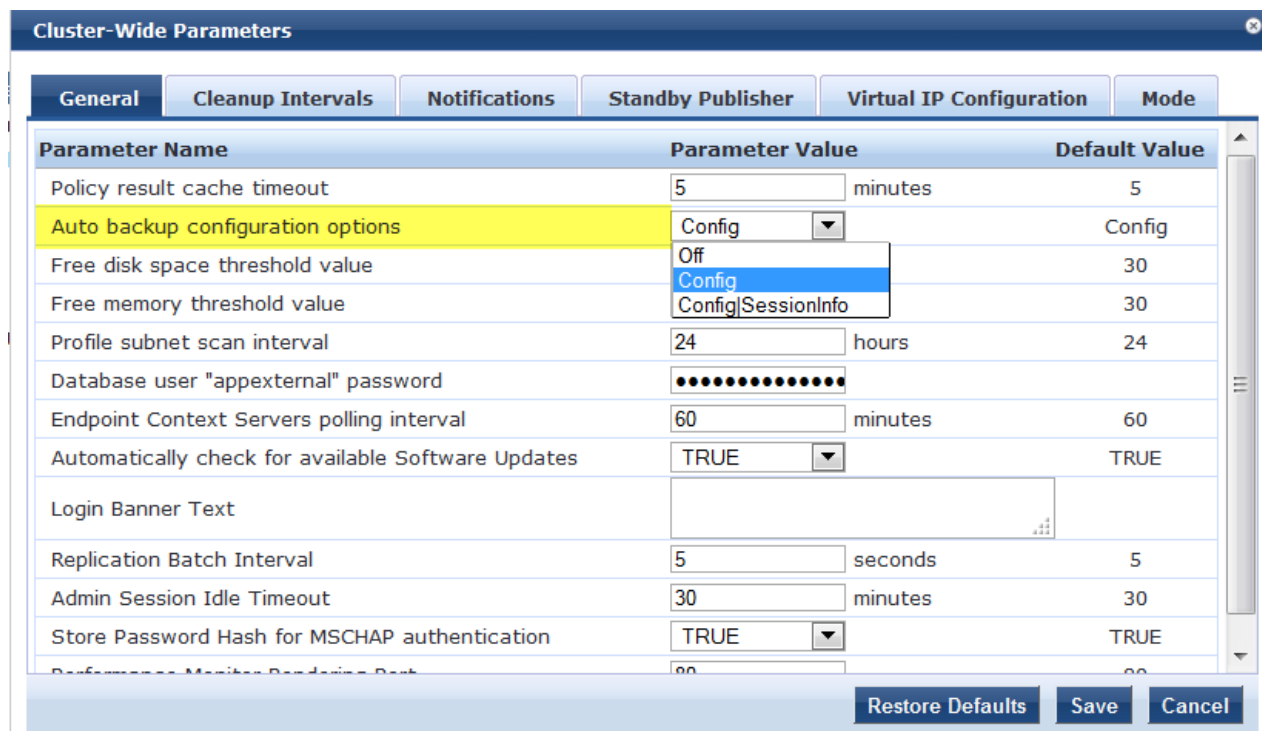
1. On the publisher node, navigate to **Administration > Server Manager > Server Configuration**.

Figure 141 Server Configuration Menu



2. From the **Server Configuration** page, choose **Cluster-Wide Parameters**.

Figure 142 Auto Backup Configuration Options



3. From the **Auto backup configuration options** drop-down, choose **Config|SessionInfo**.
4. When finished with changes to the cluster-wide parameters, click **Save**.

Using High Capacity Guest Mode

This section contains the following information:

- [Introduction](#)
- [Licensing Considerations](#)
- [EAP-PSK Protocol](#)
- [Enabling High Capacity Guest Mode](#)
- [Cleanup Intervals Settings for High Capacity Guest Mode](#)
- [Service Templates Supported](#)
- [Service Types Supported](#)
- [Authentication Methods Supported](#)

Introduction

High Capacity Guest mode supports the high-volume licensing requirements in the public-facing enterprise environment, where a large volume of unique endpoints require wireless access and the number of endpoints changes every day, such as airports, hotels, hospitals, and shopping malls (for related information, see [Licensing Considerations](#)).

When High Capacity Guest mode is enabled on a cluster, the count of unique endpoints is reset every day, providing the ability for a node to support double the number of guest accounts, regardless of whether it's a hardware or virtual appliance.

ClearPass Insight

High Capacity Guest mode requires that the W-ClearPass Insight reporting tool must be enabled on at least one node in the cluster. For instructions on enabling Insight, as well as guidance as to where Insight should be enabled in the cluster, see [Deploying W-ClearPass Insight in a Cluster on page 152](#).

Restrictions

When High Capacity Guest mode is enabled in a cluster, the following restrictions apply:

- Configuration settings cannot be moved from one cluster to another cluster that operates in High Capacity Guest mode.
- Restoring configuration data is allowed only with the backup files from W-ClearPass servers that have High Capacity Guest mode enabled.
- Use case-related settings other than High Capacity Guest mode settings are restricted.
- Access to OnGuard and OnBoard is restricted.
- Default cleanup interval values are reset (see [Cleanup Intervals Settings for High Capacity Guest Mode](#) for details).
- Only Guest application licenses are allowed.

Features Disabled Under High Guest Mode

In allowing double the number of licensed guest users, the following W-ClearPass features are disabled:

- W-ClearPass Onboard
- W-ClearPass OnGuard
- Performing posture checks on endpoints
- Performing audit checks on endpoints
- Service templates to configure 802.1X for both wired and wireless LANs
- The following EAP methods are disabled: FAST, GTC, MSCHAPv2, PEAP, TLS, TTLS

Licensing Considerations

You can add only guest licenses to High Capacity Guest mode. After enabling High Capacity Guest mode, you cannot add enterprise licenses.

If the number of licenses used exceeds the number of licenses purchased, a warning message appears four months after the number is exceeded.

The number of licenses used is based on the daily moving average.

In High Capacity Guest mode, a maximum of 2x guest licenses are allowed. For example, if you use the W-ClearPass 25K hardware appliance (CP-HW-25K) that supports 25,000 licenses, a maximum of 50,000 licenses would be allowed in High Capacity Guest mode.



The additional guest licenses that High Capacity Guest mode provides must be purchased and applied.

An additional consideration to keep in mind is that the W-ClearPass Policy AAA licensing is reset on a daily basis. For example, if you purchase 8,000 Guest licenses for a W-ClearPass 5K hardware appliance (CP-HW-5K), you would be entitled to process 8,000 unique endpoints/guests per day.

EAP-PSK Protocol

When High Capacity Guest mode is enabled, EAP-PSK, a preshared key extensible authentication protocol is available. EAP-PSK is a method for mutual authentication and session key derivation using a preshared key (PSK). EAP-PSK provides a protected communication channel for both parties to communicate over when mutual authentication is successful.

EAP-PSK is well suited to a CPPM node running in High Capacity Guest mode. It simplifies the deployment of a guest network that is "open" in that the user ID and password are the same for each user, but secure as each guest/endpoint uses a unique per-endpoint Wi-Fi Protected Access (WPA) preshared key. The client doesn't need to support anything more than WPA-PSK.

Enabling High Capacity Guest Mode



When nodes are enabled for this mode, they can only be clustered with nodes that are also in High Capacity Guest mode. Adding a High Capacity Guest mode-enabled node to a cluster in which High Capacity Guest mode is not enabled on all the other nodes is not supported.

To enable High Capacity Guest mode:

1. Enable W-ClearPass Insight on at least one node in the cluster.
2. Navigate to **Administration > Server Manager > Server Configuration > Cluster-Wide Parameters**.
3. Select the **Mode** tab.

The screen shown in [Figure 143](#) appears.

Figure 143 *Enabling High Capacity Guest Mode*

Parameter Name	Parameter Value	Default Value
High Capacity Guest Mode	TRUE	FALSE

The High Capacity Guest (HCG) Mode is intended for deployment in high volumes of guest access.

Enabling HCG Mode will restrict the following -

- ClearPass Onboard and OnGuard applications will be disabled
- Only Guest application licenses can be added
- Posture checks and Host Audit checks are not allowed
- RADIUS-based authentication methods that are disabled - EAP-FAST, EAP-GTC, EAP-MSCHAPv2, EAP-PEAP, EAP-TLS, EAP-TTLS
- Service Templates to configure 802.1X for wired / wireless or perform Posture checks are not allowed

HCG Mode requires ClearPass Insight to be enabled on at least one node in the cluster

4. To enable High Capacity Guest mode, select **TRUE** from the drop-down, then click **Save**.

You receive the message:

<n> parameters updated successfully...Please refresh to continue.

- Refresh the page.

Cleanup Intervals Settings for High Capacity Guest Mode

When you enable High Capacity Guest mode, the values for the **Cleanup Intervals** parameters are set automatically to ensure that W-ClearPass can support the significantly higher numbers of guests by making sure the amount of data stored in W-ClearPass is kept to a minimum (as shown in [Figure 144](#)).

To see the Cleanup Interval settings for High Capacity Guest mode:

- Navigate to the **Cluster-Wide Parameters > Cleanup Intervals** tab.
The Cleanup Intervals dialog opens.

Figure 144 High Capacity Guest Mode Values for the Cleanup Intervals Parameters

Parameter Name	Parameter Value	Default Value
Maximum inactive time for an endpoint	0 days	0
Cleanup interval for Session log details in the database	3 days	7
Cleanup interval for information stored on the disk	7 days	7
Known endpoints cleanup interval	3 days	0
Unknown endpoints cleanup interval	3 days	0
Expired guest accounts cleanup interval	10 days	365
Profiled Unknown endpoints cleanup interval	3 days	0
Static IP endpoints cleanup option	FALSE	FALSE
Old Audit Records cleanup interval	10 days	7
Profiled Known endpoints cleanup option	TRUE	FALSE

[Table 28](#) shows the value for each Cleanup Intervals parameter while in High Capacity Guest mode.

Table 28: Cleanup Interval Parameter Values in High Capacity Guest Mode

Cleanup Intervals Parameters	Values for HCG Mode
Maximum inactive time for an endpoint	HGC mode value: 0 days
Cleanup interval for Session log details in the database	HGC mode value: 3 days
Cleanup interval for information stored on the disk.	HGC mode value: 7 days
Known endpoints cleanup interval	HGC mode value: 3 days

Cleanup Intervals Parameters	Values for HCG Mode
Unknown endpoints cleanup interval	HGC mode value: 3 days
Expired guest accounts cleanup interval	HGC mode value: 10 days
Profiled endpoints cleanup interval	HGC mode value: 3 days
Static IP endpoints cleanup option	HGC mode value: FALSE
Old Audit Records cleanup interval	HGC mode value: 10 days
Profiled Known endpoints cleanup option	HGC mode value: TRUE

2. Click **Cancel** to exit.

Service Templates Supported

The following service templates are supported when High Capacity Guest mode is enabled:

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

Service Types Supported

The following service types are supported when High Capacity Guest mode is enabled:

- MAC Authentication
- RADIUS Authorization
- 1RADIUS Enforcement
- RADIUS Proxy
- Dell W-Series Application Authentication
- Dell W-SeriesApplication Authorization
- TACACS+ Enforcement
- Web-based Authentication
- Web-based Open Network Access

Authentication Methods Supported

The following authentication methods are used in service templates in High Capacity Guest mode:

- PAP
- CHAP

- MSCHAP
- EAP_MD5
- MAC_AUTH
- AUTHORIZE
- EAP_PEAP_PUBLIC

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 required and optional 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 make-subscriber 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.



WARNING

Running this command erases the Policy Manager configuration and resets the database to its default configuration—all the configured data will be lost.



NOTE

When running this command, do not close the shell or interrupt the command execution.

Syntax and Example

```
cluster reset-database
```

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.



NOTE

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
```

This chapter describes how to configure a 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:

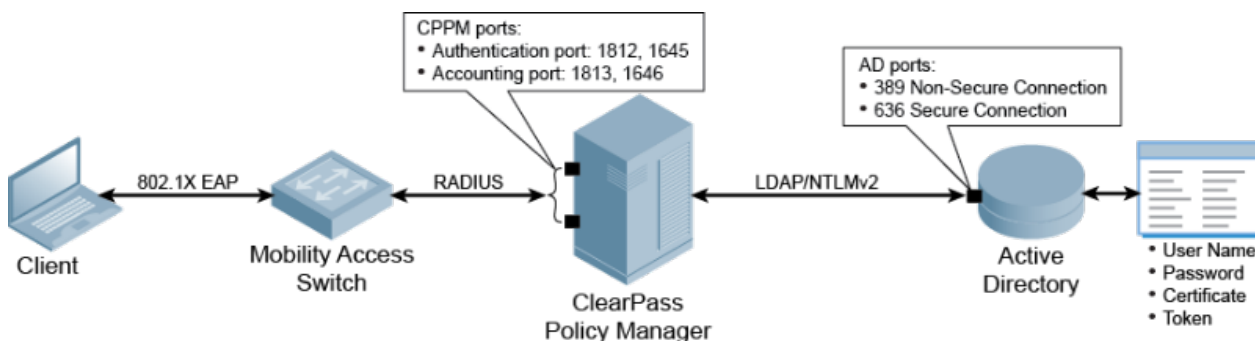
- [About Defining Wired 802.1X Authentication](#)
- [Configuring Authentication with a RADIUS Server](#)
- [Authentication Terminated on the Mobility Access Switch](#)
- [Configuring Access Control Lists](#)

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 145](#) shows the network traffic flow for wired clients that connect to an Dell Mobility Access Switch or a third-party switch and perform 802.1X authentication to the W-ClearPass Policy Manager server.

Figure 145 Traffic flow for 802.1X Wired Authentication with Active Directory



The configuration process is as follows:

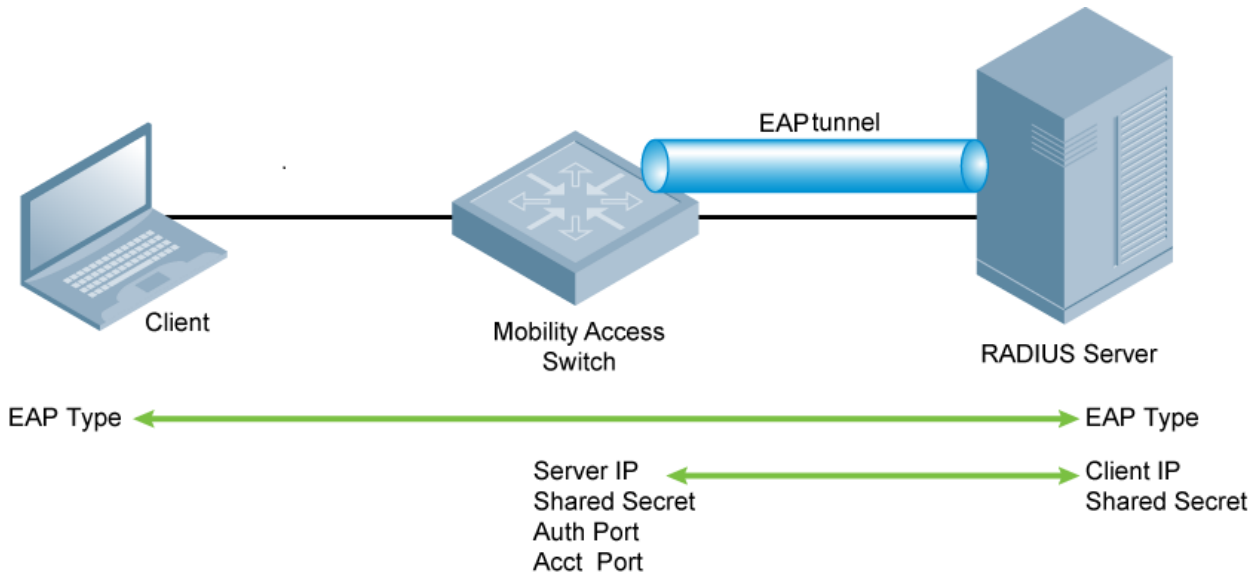
1. Define an external RADIUS server or create an internal database.
2. Define a server group and apply one of the servers above to this server group.
3. Create 802.1X authentication profiles.
4. Apply the server group to each of the 802.1X authentication profiles.
5. Apply the 802.1X authentication profiles 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 146](#)). Therefore, the network authentication and encryption configured must be the same on both the client and the Mobility Access Switch.

Figure 146 802.1x 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: 1812 .
Accounting port	3. Enter the Accounting port number on the authentication server. Default: 1813 .

- 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.

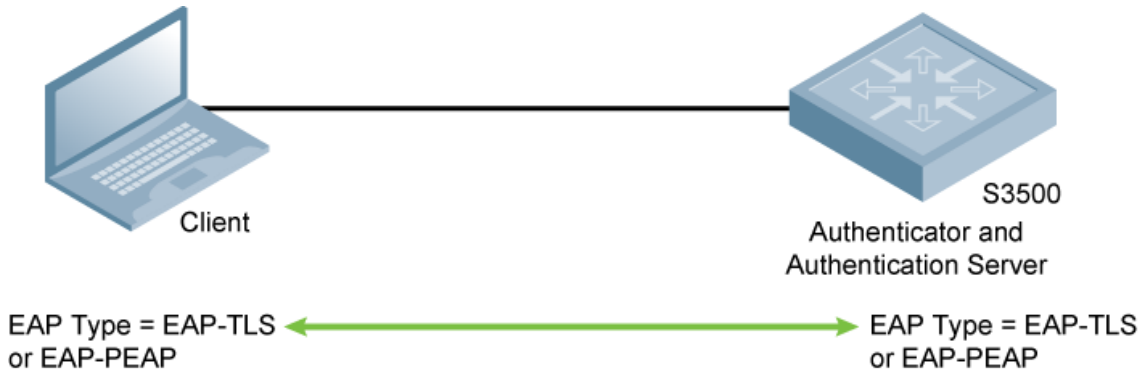


Additional information on EAP types supported in a Windows environment for Microsoft supplicants and the authentication server is available at [http://technet.microsoft.com/en-us/library/cc782851\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc782851(WS.10).aspx).

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 147 802.1x 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 166](#).
- For the CLI example, see [Examples of Common 802.1X Configuration Tasks Via the CLI on page 176](#).

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**
Ether-type ACLs filter based on the *Ether-type* field in the frame header. Ether-type 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:

```
(DellSwitch) (config) #'''ip access-list stateless STATELESS'''  
(DellSwitch) (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:

```
(DellSwitch) (config) #'''interface gigabitethernet 0/0/8'''  
(DellSwitch) (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:


```
(DellSwitch) (config) #'''user-role EMPLOYEE_1'''  
  
(DellSwitch) (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.

Verifying Stateless ACL Configuration

To verify a stateless ACL configuration:

```
(DellSwitch) #'''show ip access-list STATELESS'''
```

Verifying Stateless ACL Traffic Hits

To verify stateless traffic hits:

```
(DellSwitch) #'''show acl hits'''
```

Verifying Stateless ACL Operation

To verify stateless ACL operation:

```
(DellSwitch) # '''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
```

```
802.1X Authentication Profile "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 148 Enabling the Enforce Machine Authentication Option

802.1X Authentication Profile > dot1x_prof-sxy02 Show Reference Save As Reset

Basic Advanced

Max authentication failures	<input type="text" value="0"/>
Enforce Machine Authentication	<input type="checkbox"/>
Machine Authentication: Default Machine Role	guest ▼
Machine Authentication: Default User Role	guest ▼
Reauthentication	<input type="checkbox"/>
Termination	<input type="checkbox"/>
Termination EAP-Type	<input type="checkbox"/> eap-tls <input type="checkbox"/> eap-peap
Termination Inner EAP-Type	<input type="checkbox"/> eap-mschapv2 <input type="checkbox"/> eap-gtc
Enforce Suite-B 128 bit or more security level Authentication	<input type="checkbox"/>
Enforce Suite-B 192 bit security level Authentication	<input type="checkbox"/>

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 31](#) describes role assignment based on the results of the machine and user authentications.

Table 31: 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 take 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 32](#) describes VLAN assignment based on the results of the machine and user authentications when VLAN derivation is used.

Table 32: 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"> VLAN configured on the interface. VLAN configured under initial role.
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"> VLAN configured on the interface. VLAN configured under machine authentication default user role.
Passed	Failed	Machine authentication succeeds and user authentication has not been initiated.	<ul style="list-style-type: none"> VLAN configured on the interface. VLAN configured under machine authentication default user role.
Passed	Passed	Both machine and user are successfully authenticated.	<ul style="list-style-type: none"> Derived VLAN. VLAN configured on the interface.

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 W-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**.

Figure 149 Adding a Generic LDAP Authentication Database

Configuration » Authentication » Sources » Add

Authentication Sources

General	Primary	Attributes	Summary
Name:	<input type="text" value="LDAP1"/>		
Description:	<input type="text"/>		
Type:	Generic LDAP		
Use for Authorization:	<input checked="" type="checkbox"/> Enable to use this Authentication Source to also fetch role mapping attributes		
Authorization Sources:	<input type="text"/>		Remove View Details
	-- Select --		
Server Timeout:	<input type="text" value="10"/> seconds		
Cache Timeout:	<input type="text" value="36000"/> seconds		
Backup Servers Priority:	<input type="text"/>		Move Up Move Down
	<input type="text"/>		Add Backup Remove

3. Enter the values for these parameters as described in [Table 33](#).

Table 33: General Page Parameters for Generic LDAP Database

Parameter	Action/Description
Name	1. Enter the name of the LDAP authentication source.
Description	2. Provide the additional information that helps to identify the LDAP authentication source.
Type	3. Select Generic LDAP .
Use for Authorization	When Use for Authorization is enabled, W-ClearPass can use this authentication source to fetch role-mapping attributes. This option is enabled by default.
Backup Servers Priority	4. To add a backup server in the event the main server goes down, click Add Backup . NOTE: Dell recommends setting up one or more backup servers.
Authorization Sources	Specifies additional sources from which role-mapping attributes may be fetched. 5. Select a previously configured authentication source from the drop-down list. 6. To add authentication source to the list of authorization sources, click Add . To remove the authentication source from the list, click Remove . If Policy Manager authenticates the user or device from this authentication source, 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 36000 seconds (one hour).
Backup Servers Priority	7. To add a backup server, click Add Backup . If the Backup 1 tab appears, you can specify connection details for a backup server. <ul style="list-style-type: none"> To remove a backup server, select the server name and click Remove. To change the server priority of the backup servers, select Move Up or Move Down. This is the order in which Policy Manager attempts to connect to the backup servers when the primary server is unreachable.
	8. When satisfied with these settings, click Next . The Authentication Sources Primary page opens.

Primary Page

Figure 150 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
Connection Details			
Hostname:	<input type="text" value="LDAP1"/>		
Connection Security:	<input type="text" 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="text"/>		
Base DN:	<input type="text"/>		Search Base Dn
Search Scope:	<input type="text" 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="text" value="Cleartext"/>		
Password Header:	<input type="text"/>		
User Certificate :	<input type="text" value="userCertificate"/>		

Table 34: Primary Parameters for an LDAP Authentication Source

Parameter	Action/Description
Hostname	<ol style="list-style-type: none"> Enter the name or IP address of the LDAP server you're going to use for authentication. Note that most domain controllers are also LDAP servers. W-ClearPass uses LDAP to talk to the domain controller.
Connection Security	<ol style="list-style-type: none"> Set Connection Security to: LDAP over SSL. This enables the secure sockets layer (SSL) cryptographic protocol to connect to your Active Directory. Selecting LDAP over SSL automatically populates the <i>Port</i> field to 636. NOTE: In a production environment, security is a concern because when W-ClearPass binds to an LDAP server, it submits the username and password for that account over the network under clear text unless you protect it using Connection Security and set the port to 636. NOTE: To ensure successful authentication, be sure to add the CA certificate of the LDAP server to the Certificate Trust List. For more information, refer to Importing the Root CA Files to the Certificate Trust List.
Port	<ol style="list-style-type: none"> Specify the TCP port at which the LDAP server is listening for connections. For a single domain LDAP Domain Service: <ul style="list-style-type: none"> Default port for LDAP: 389 Default port for LDAP over SSL: 636 When you set the <i>Connection Security</i> field to AD over SSL, this port is automatically set to 636.

Parameter	Action/Description
	<p>For a multi-domain LDAP Domain Service forest, the default ports for the global catalog are:</p> <ul style="list-style-type: none"> • Default port without SSL: 3268 • Default port with SSL: 3269
Verify Server Certificate	4. Enable this option to verify the Server Certificate for a secure connection.
Bind DN	<p>5. 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><code>CN=Administrator,CN=Users,DC=mycompany,DC=com</code></p> <p>NOTE: You may need to get the Bind DN from the LDAP 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> <ul style="list-style-type: none"> • For a single domain LDAP Domain Service, the Bind DN entry must be located in the same branch and below the Base DN. • 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. <p>W-ClearPass fills in the domain portion of the Bind DN.</p> <p>6. Specify the username.</p> <p>W-ClearPass also populates the <i>Base DN</i>, and the <i>NetBIOS Domain Name</i> fields.</p> <p>For related information, see LDAP Authentication Source Configuration.</p>
Bind Password	<p>This is the text box for the Active Directory password for the account that can search for users.</p> <p>7. Enter the Bind password.</p> <p>NOTE: The Bind password is the same password used in association with the Bind DN user account.</p>
Base DN	<ul style="list-style-type: none"> • 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: <code>DC=mycompany,DC=com</code> <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>NOTE: The Base DN value that is automatically populated in this instance is <i>not</i> the best practice Base DN value.</p>

Parameter	Action/Description
	<p>Dell 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> <p>8. To browse the LDAP directory hierarchy, click Search Base DN. The LDAP Browser opens.</p> <p>9. Navigate to the DN you want to use as the Base DN.</p> <p>10. Click on the appropriate node in the tree structure to select it as a Base DN.</p> <ul style="list-style-type: none"> • For a multi-domain Active Directory Domain Service (AD DS) forest, the appropriate action is to leave the Base DN text box blank. <p>NOTE: 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 Search Base DN.</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>11. Select the Search Scope.</p> <ul style="list-style-type: none"> • Subtree Search: Searches every object and sub-object in the LDAP directory. • One-Level Search: Looks directly under the Base DN. • Base Object: Searches any object under the Base DN.
LDAP Referrals	<p>Dell 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>12. 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	<p>13. Enter the name of the attribute in the user record from which the user password can be retrieved.</p>
Password Type	<p>14. Specify the password type: Cleartext, NT Hash, LM Hash, SHA1, SHA256, MD5.</p>
Password Header	<p>Oracle's LDAP implementation prepends a header to a hashed password string.</p> <p>15. 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	<p>16. 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.</p>
	<p>17. 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.</p>

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, MySQL, 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 151 *General Page: Generic SQL Authentication Database*

The screenshot shows the 'Authentication Sources' configuration page in a web interface. The breadcrumb path is 'Configuration » Authentication » Sources » Add'. The page title is 'Authentication Sources'. There are four tabs: 'General' (selected), 'Primary', 'Attributes', and 'Summary'. The form fields are as follows:

- Name:** An empty text input field.
- Description:** A large empty text area.
- Type:** A dropdown menu with 'Generic SQL DB' selected.
- Use for Authorization:** A checkbox labeled 'Enable to use this Authentication Source to also fetch role mapping attributes' which is checked.
- Authorization Sources:** A list box containing '-- Select --'. To its right are 'Remove' and 'View Details' buttons.
- Cache Timeout:** A text input field with '36000' and the label 'seconds'.
- Backup Servers Priority:** A list box with 'Move Up', 'Move Down', 'Add Backup', and 'Remove' buttons.

At the bottom of the form, there is a blue bar with a left-pointing arrow and the text 'Back to Authentication Sources'. On the right side of this bar are three buttons: 'Next >', 'Save', and 'Cancel'.

3. Enter the information for each of the required parameters as described in [Table 35](#).

Table 35: 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 Generic SQL DB .
Use for Authorization	4. Leave the Use for Authorization setting enabled. When Use for Authorization is enabled, W-ClearPass can use this authentication 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 Add Backup . NOTE: Dell 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"> • Select a previously configured authentication source from the drop-down list. • To add authentication source to the list of authorization sources, click Add. • To remove the authentication source from the list, click Remove. <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>
Cache Timeout	7. Specify the number of seconds for the 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	8. To add a backup server, click Add Backup . If the Backup 1 tab appears, you can specify connection details for a backup server. <ul style="list-style-type: none"> • To remove a backup server, select the server name and click Remove. • To change the server priority of the backup servers, select Move Up or Move Down. <p>This is the order in which Policy Manager attempts to connect to the backup servers when the primary server is unreachable.</p>
	9. When satisfied with these settings, click Next . The Authentication Sources Primary page opens.

Primary Page

Figure 152 Primary Page: Generic SQL Authentication Source

Configuration » Authentication » Sources » Add

Authentication Sources

General Primary Attributes Summary

Connection Details

Server Name:

Port (Optional): (Specify only if you want to override the default value)

Database Name:

Login Username:

Login Password:

Timeout: seconds

ODBC Driver:

Password Type:

[Back to Authentication Sources](#)

10. Enter the information for each of the required parameters as described in [Table 36](#).

Table 36: 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	Select the ODBC driver (Postgres, Oracle11g, or MSSQL) to connect to the database. NOTE: MySQL is supported in versions 6.0 and later. Dell does not ship MySQL drivers by default. If you require MySQL, contact dell.com/support to get the required patch. This patch does not persist across upgrades. If you are using MySQL, you should contact support before upgrading.
Password Type	Specify how the user password is stored in the database:

Parameter	Action/Description
	<ul style="list-style-type: none"> • Cleartext : Password is stored as clear, unencrypted text. • NT Hash: Password is stored with an NT hash using MD4. • LM Hash : Password is stored with a LAN Manager Hash using DES. • SHA: Password is stored with a Secure Hash Algorithm (SHA) hash. • SHA256: Password is stored with an SHA-256 hash function.

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 153 Attributes Page: Generic SQL Authentication Source

12. Enter the information for each of the required parameters as described in [Table 37](#).

Table 37: Attributes Page Parameters for Generic SQL Database

Parameter	Action/Description
Filter Name	Enter the name of the filter.
Attribute Name	Specify the name of the SQL database attributes defined for this filter.
Alias Name	Specify an alias name for each attribute name selected for the filter.
Enabled As	Optionally, indicate 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 Configure Filter page (for details, see the next section, Defining a Filter Query).

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 154 Configure Filter Page: Generic SQL Authentication Source

The screenshot shows the 'Configure Filter' window. The 'Filter Name' is 'Authentication'. The 'Filter Query' is a SQL query: `SELECT user_credential(password) AS User_Password, CASE WHEN enabled = FALSE THEN 225 WHEN ((start_time > now()) OR ((expire_time is not null) AND (expire_time <= now()))) THEN 226`. Below the query is a table with the following data:

Name	Alias Name	Data type	Enabled As
1. sponsor_name	Owner	String	-
2. Click to add...			

3. Enter the information for each of the required parameters as described in [Table 38](#).

Table 38: 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	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.

Parameter	Action/Description
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

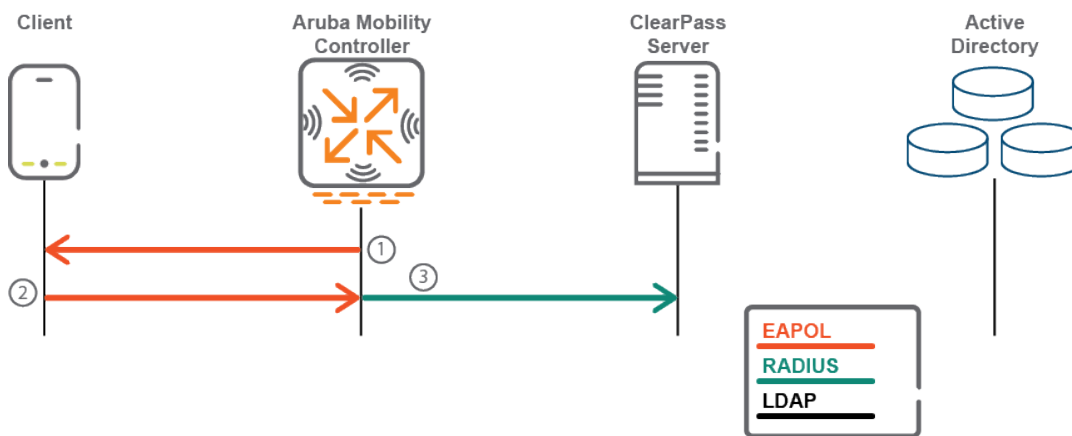
[Table 39](#) describes how a typical 802.1X authentication session flows when using W-ClearPass as the authentication server with Microsoft Active Directory as the back-end user identity repository.

- 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 Dell Mobility Controller or an Instant Access Point (AP), which controls access to a network resource.
- The term **authentication server** refers to the W-ClearPass Policy Manager server, which processes the authentication requests and provides either an accept or reject response.

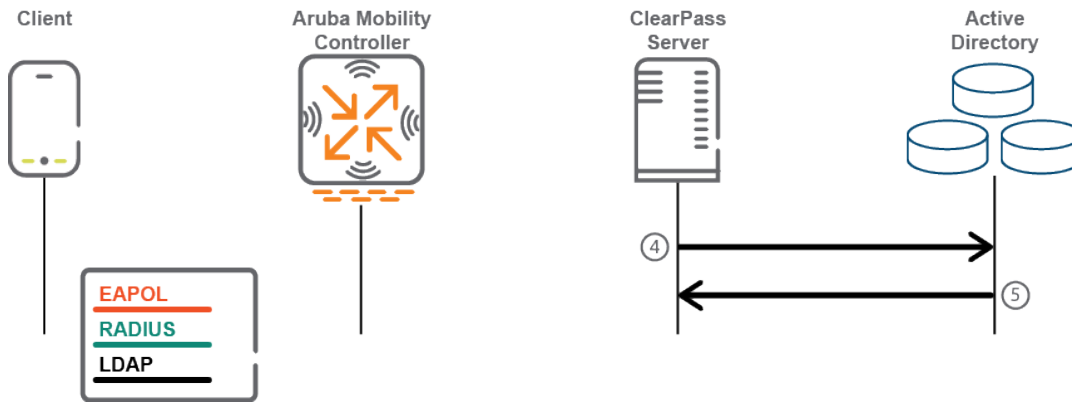
Each section of [Table 39](#) is followed by a diagram that illustrates the communication steps between the devices described in the table. The numbers of each step in the table correspond to the numbers assigned to the handshake sequences in the accompanying illustrations.

Table 39: Detailed Sequence of the EAP-PEAP-Active Directory Handshake Exchange

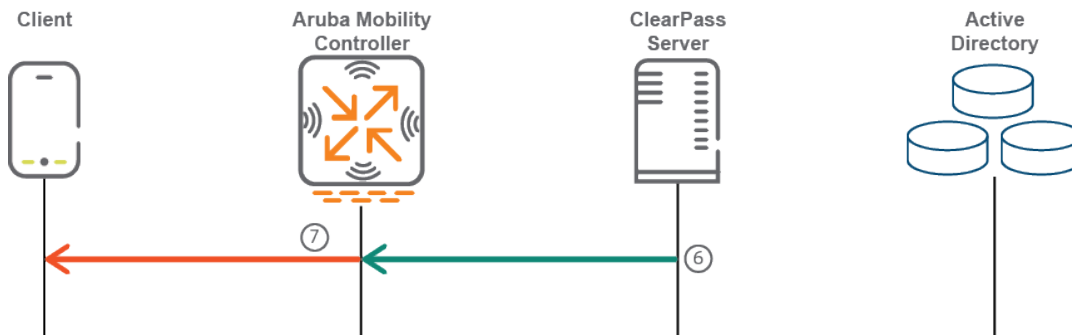
Extensible Authentication Protocol over LAN (EAPOL) Start	
1	The authenticator sends an EAP-Request for the identity of the connecting supplicant (client device).
2	The supplicant responds to the authenticator with an EAP Identity Response that contains the identity (username) used for authentication. 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 (W-ClearPass Policy Manager).



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.



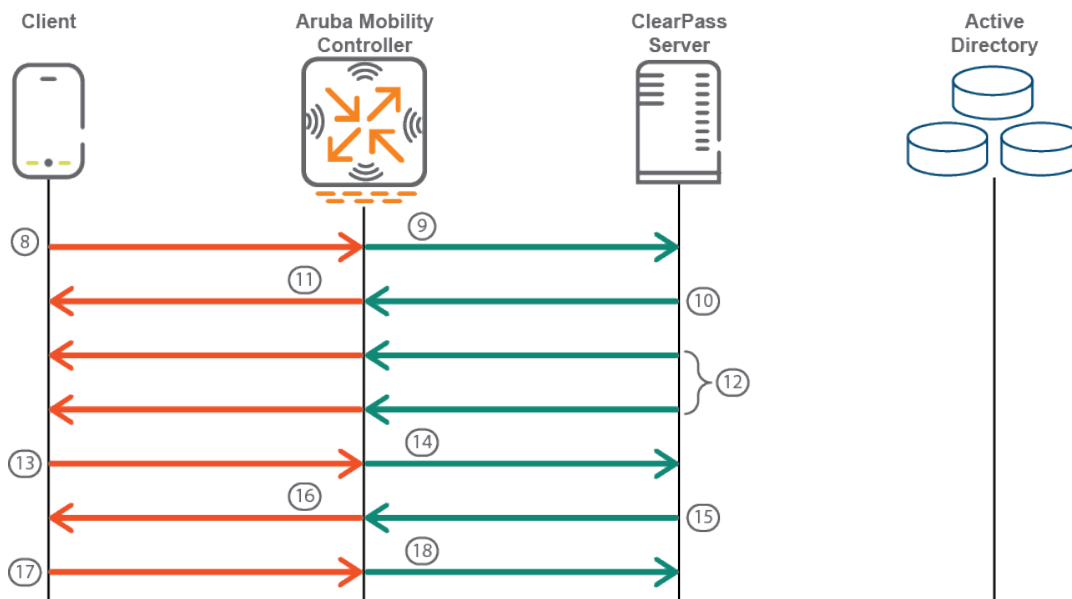
EAPOL	
6	The authentication server responds to the supplicant through the authenticator with an EAP-Request message indicating that it would like to initiate EAP-PEAP.
7	The authenticator passes the EAP-Request message to the supplicant.



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.

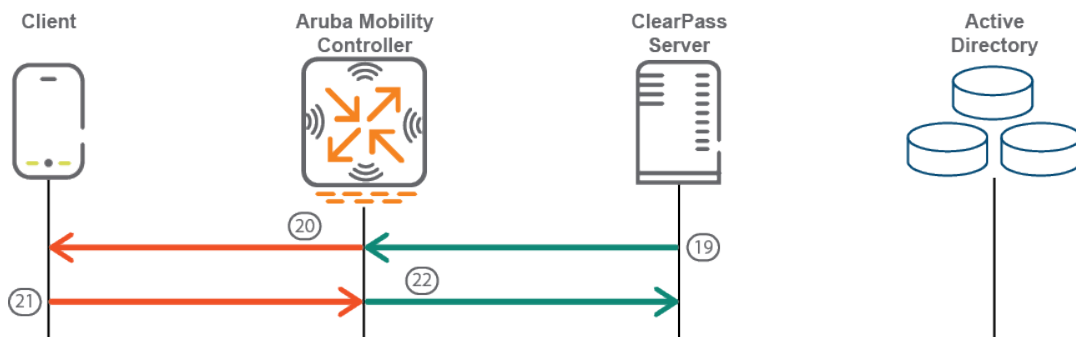


Inner EAP MSCHAPv2

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.
----	--

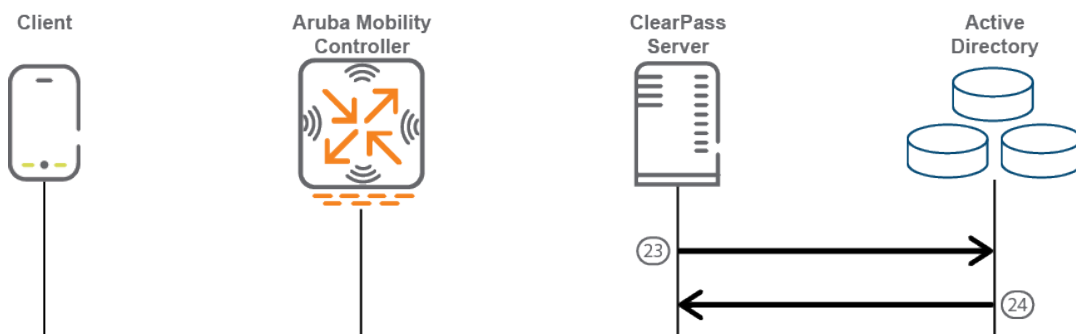
Inner EAP MSCHAPv2

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.



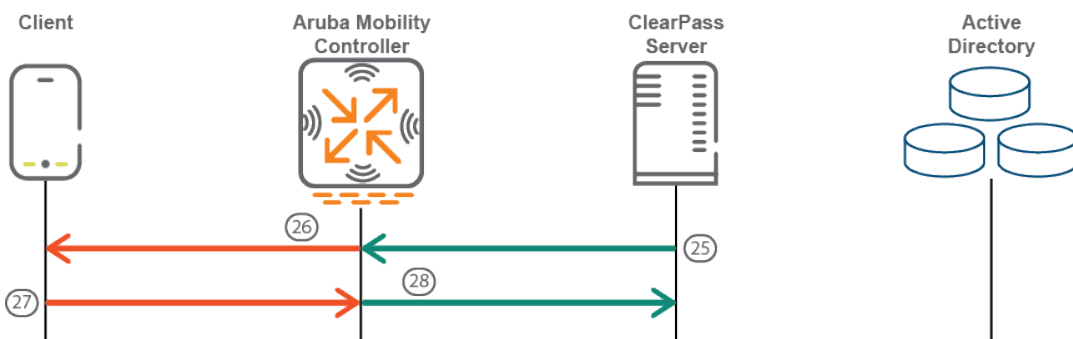
Active Directory

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.



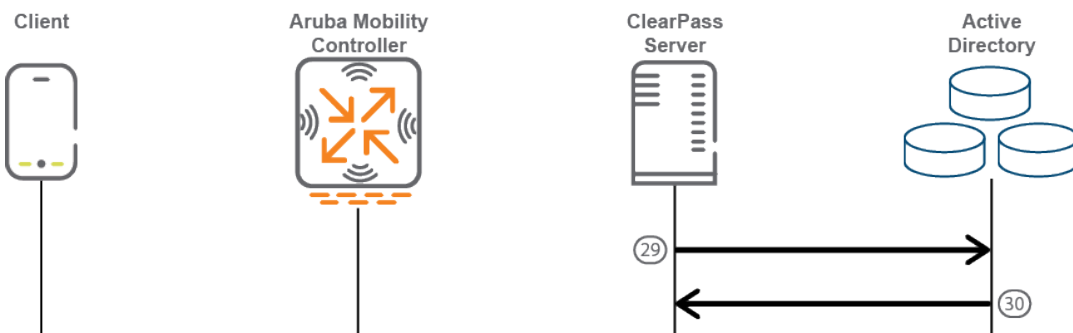
Inner EAP MSCHAPv2

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.



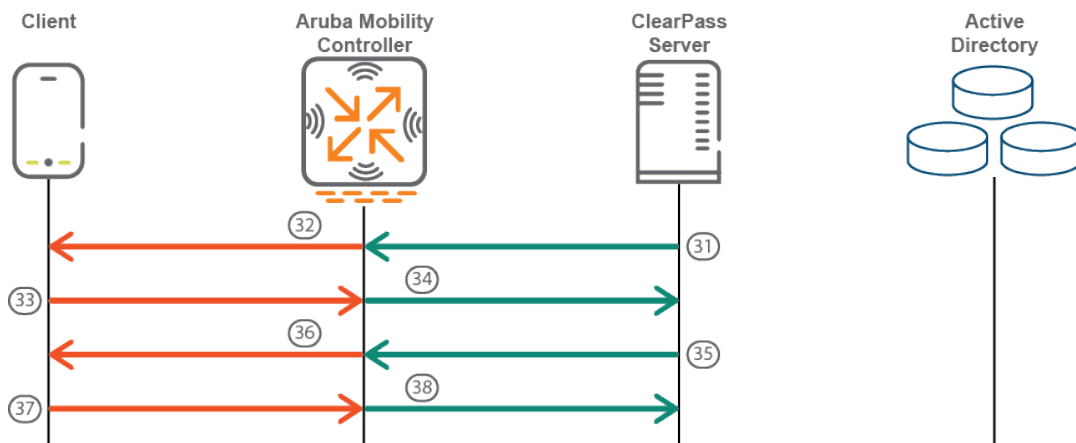
Active Directory

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.



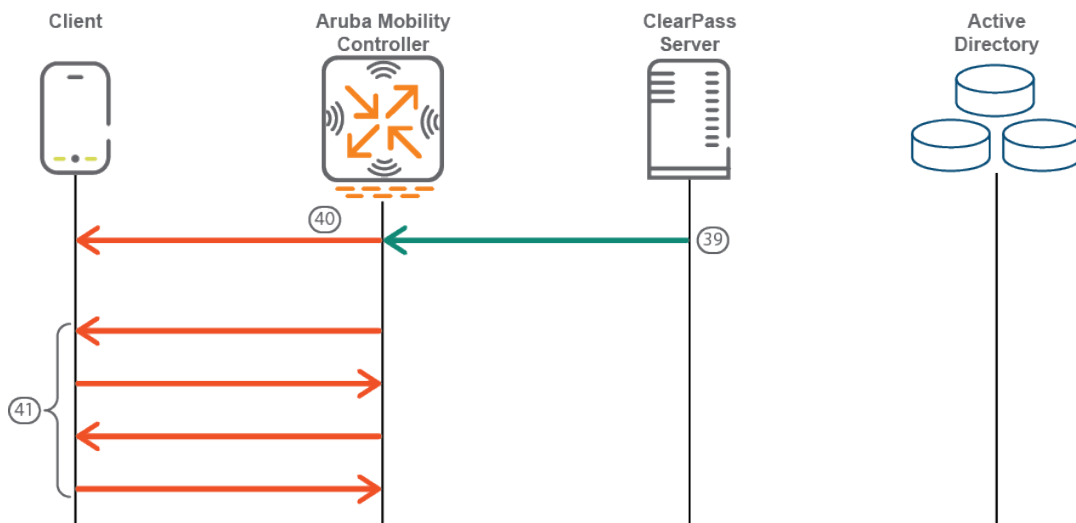
Inner EAP MSCHAPv2

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

39	The authentication server sends a RADIUS access-accept message to the authenticator with an EAPOL success message along with the key material.
40	The authenticator sends an EAPOL success message to the supplicant.
41	The authenticator and supplicant complete a four-way handshake to start the flow of encrypted wireless traffic.



This chapter includes the following information:

- [W-ClearPass Configuration API Overview](#)
- [W-ClearPass Configuration API Methods](#)
- [W-ClearPass Configuration API Examples](#)
- [API Error Handling](#)
- [About the API Explorer](#)

W-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 W-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 W-ClearPass Configuration API allows you to configure or modify the entities in W-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 W-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 W-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 W-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 W-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.

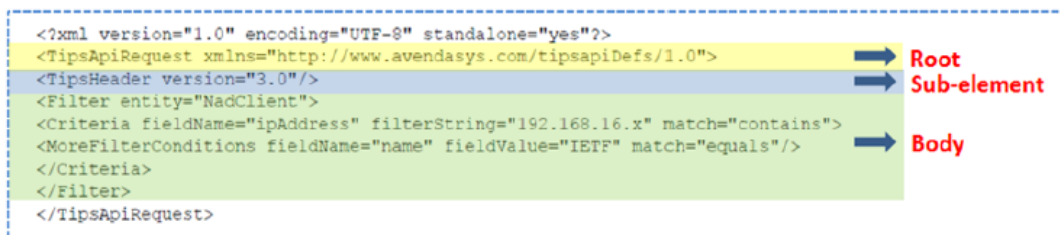
XML Data Structure

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.

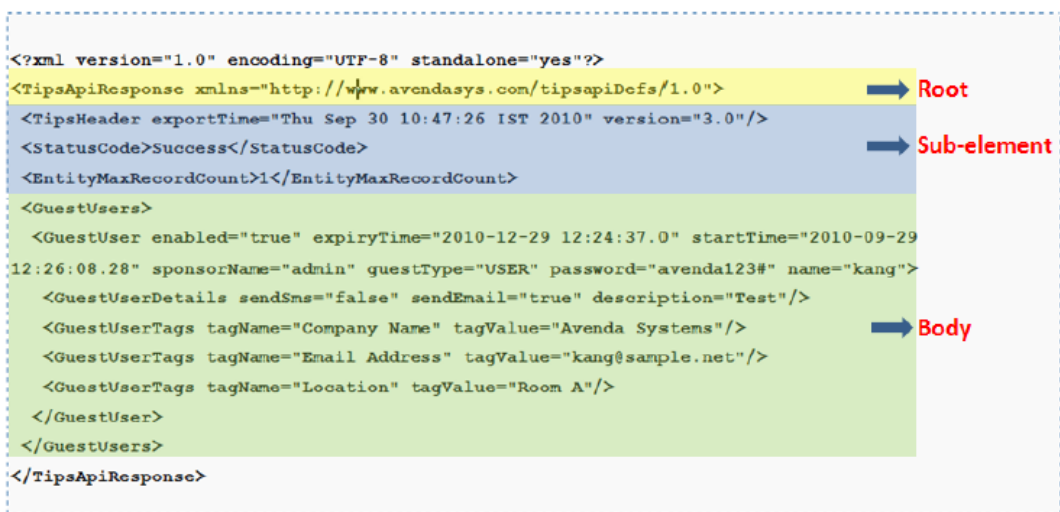
[Figure 155](#) describes the structure of XML data in an XML request:

Figure 155 Structure of an XML Request



[Figure 156](#) describes the structure of XML data in an XML response:

Figure 156 Structure of an XML Response



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 recommend 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>001122aabbcc</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="3f8e0a80-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>
```

W-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 W-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 W-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 40](#) describes the **Entity Names** supported in the W-ClearPass Policy Manager Configuration API.

Table 40: 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. NOTE: 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. NOTE: 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>
</EntityOrderList>
</TipsApiRequest>
```

```
<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>

```

W-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 W-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 **StatusCode**, **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

1. 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 W-ClearPass Configuration API, Dell offers a number of other APIs that are available through the API Explorer:

Table 41: W-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 W-ClearPass Policy Manager server and select **ClearPass Guest** from **Applications** or **Quick Links**.
2. In W-ClearPass Guest, navigate to **Administration > API Services > API Clients**.
The API Clients page opens.

Figure 157 API Clients Page

ClearPass Guest Support | Help | Logout
demoadmin (IT Administrators)

Home » Administration » API Services » API Clients

API Clients

[Create API client](#)
? API Explorer

The API clients you have defined are listed below.

Filter:

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 158 *API Explorer Dialog*

API Explorer

API	Services	Versions
ApiFramework	ApiClientS	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 159](#) is the OperatorLogins API.

Figure 159 *OperatorLogins API Selected*

API Explorer – OperatorLogins-v1

[Back to API Explorer](#)

Authorization:

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**.