Dell Networking W-ClearPass 6.6 Getting Started Guide

Copyright Information

Open Source Code

This product includes code licensed under the GNU General Public License, the GNU Lesser General Public License, and/or certain other open source licenses. 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

Chapter 1

Setting Up W-ClearPass Hardware Appliances

This chapter documents the procedures for installing and configuring W-ClearPass on a hardware appliance.

About This Guide

Welcome to the *W-ClearPass Getting Started Guide*. This guide contains the following information:

- About the W-ClearPass Access Management System
- Setting Up the W-ClearPass Hardware Appliances
- Using vSphere Web Client to Install W-ClearPass on a Virtual Machine
- Using Hyper-V to Install W-ClearPass on a Virtual Appliance
- Maintaining W-ClearPass Policy Manager Services

Intended Audience

The intended audience for the *W-ClearPass Getting Started Guide* includes customers, partners, system administrators, and Dell/HP Enterprise 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, Certified W-ClearPass Professional (CCP) certification.

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

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

NOTE

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

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 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 multi-vendor 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 Mobile Device Management (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 W-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, perform 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.

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

- For W-ClearPass hardware appliance installation and deployment procedures, see Setting Up the W-ClearPass Hardware Appliances on page 9.
- For W-ClearPass virtual appliance installation and deployment procedures:
  - VMware ESX and ESXi: Using vSphere Web Client to Install W-ClearPass on a Virtual Machine on page 21
  - Microsoft Hyper-V: Using Hyper-V to Install W-ClearPass on a Virtual Appliance on page 34.

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 provides 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	The Enterprise port provides remote access to the system—whether or not there is a functioning operating system running on the appliance. This port allows you to monitor, manage, update, troubleshoot, and remediate the W-ClearPass 25K appliance from any location. **NOTE:** Available only on the CP-HW-25K appliance.

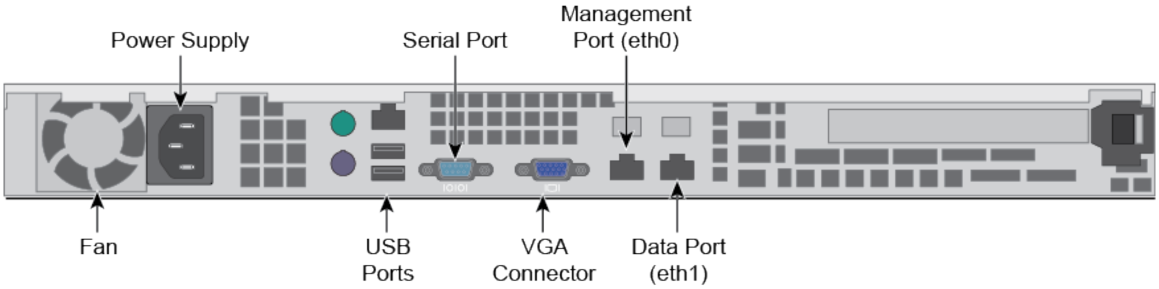
W-ClearPass Policy Manager 500 Hardware Appliance

The W-ClearPass W-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 500 GB 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-ClearPass W-Policy Manager 500 hardware appliance.

Table 2: *CP-HW-500 Specifications*

CP-HW-500 Component	Specification
CPU	Pentium G850, Dual Core, 2.9Ghz, 3 MB Cache
Memory	4 GB (2 x2 GB)
Hard drive storage	500 GB 7.3 K RPM, Serial ATA
Maximum unique endpoints	● High Capacity Guest (HGC) mode enabled: 1,000 ● HGC not enabled: 500
Maximum number of authentications per day	● 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)

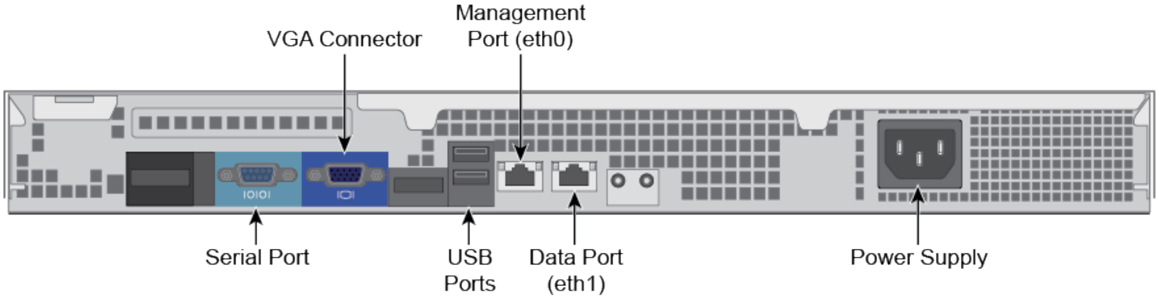
W-ClearPass Policy Manager 5K Hardware Appliance

The W-ClearPass W-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 W-Policy Manager a single virtual 1 TB drive, masking the two underlying physical drives.

Figure 2 shows the ports on the rear panel of the W-ClearPass W-Policy Manager 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 Policy Manager hardware appliance by connecting a monitor and keyboard to the hardware appliance.

Table 3 describes the specifications for the W-ClearPass W-Policy Manager 5K hardware appliance.

Table 3: *CP-HW-5K Specifications*

CP-HW- 5K Component	Specification
CPU	Xeon E3-1220 3.10 GHz, 8 M Cache, Quad Core/4T
Memory	8 GB Memory (4 x 2 GB)
Hard disks	(2) 1 TB 7.2K RPM SATA 3 Gbps
• RAID controller • RAID configuration	• PERC H200 • 1
OOB management	Baseboard Management Controller (BMC)
Maximum unique endpoints	• High Capacity Guest (HGC) mode enabled: 10,000

CP-HW- 5K Component	Specification
	- HGC not enabled: 5,000
Maximum number of authentications per day	- 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 300 GB 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.

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

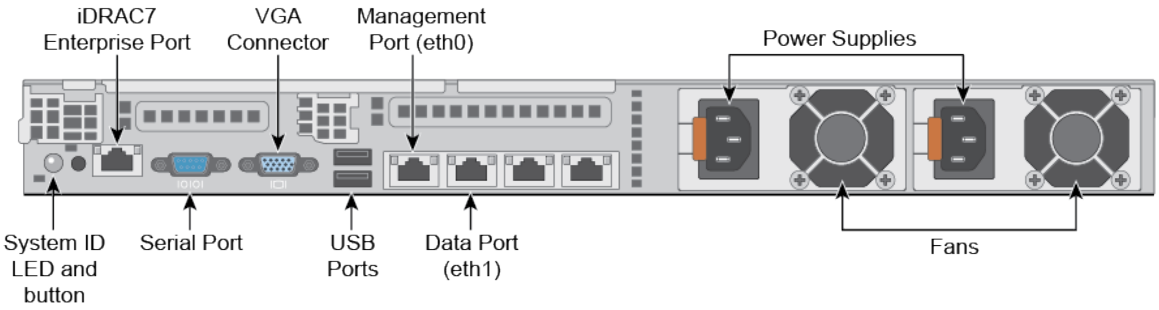


Table 4 describes the specifications for the W-ClearPass Policy Manager 25K hardware appliance.

Table 4: *CP-HW-25K Specifications*

CP-HW-25K Component	Specification
CPUs	(2) Xeon X5650 2.66 Ghz, 12 M Cache, Turbo, HT
Memory	48 GB Memory (12 x 4 GB)
Hard disks	(4) 300 GB 10 K RPM Serial-Attach SCSI 6 Gbps
Maximum unique endpoints	● High Capacity Guest (HGC) mode enabled: 50,000 ● HGC not enabled: 25,000
Maximum number of authentications per day	● High Capacity Guest (HGC) mode enabled: 2 million ● HGC not enabled: 1 million
● RAID controller ● RAID configuration	● 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	
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 Values*

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 *not* in the same subnet as the Management port IP address.
Data port subnet mask (optional)	
Data port gateway (optional)	
Primary DNS	
Secondary DNS	
NTP server (optional)	

Configuring the 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**.

NOTE

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 18

   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.

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

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

   b. To set the date and time by configuring the NTP server, use the primary and secondary NTP server information you entered in Table 5.

7. **Apply the configuration**.

   a. To apply the configuration, press **Y**.

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

Configuration on the hardware appliance console is now complete. The next task is to activate W-ClearPass Policy Manager.

Activating W-ClearPass

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

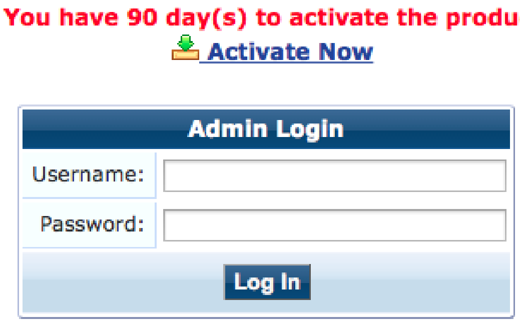
1. After the configuration has been applied at the virtual appliance console, open a web browser and go to the W-ClearPass Policy Manager management interface:

   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.

2. 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*



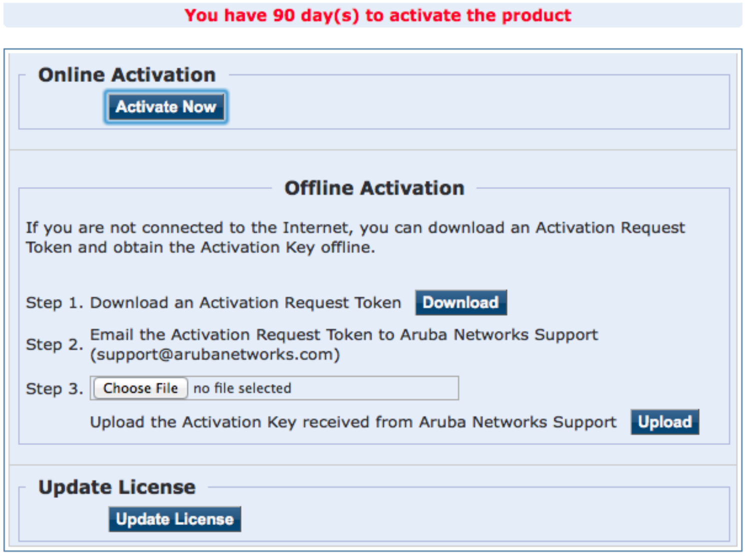
You have 90 day(s) to activate the product

3. 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 Dell 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*



You have 90 day(s) to activate the product

If you are not connected to the Internet, you can download an Activation Request Token and obtain the Activation Key offline.

Step 1. Download an Activation Request Token

Step 2. Email the Activation Request Token to Aruba Networks Support (support@arubanetworks.com)

Step 3. Choose File no file selected

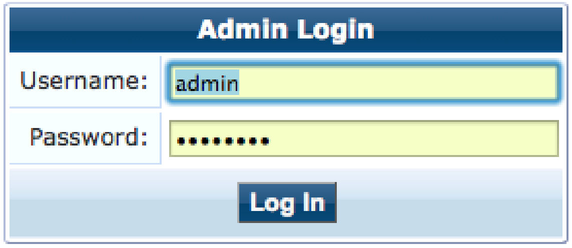
Upload the Activation Key received from Aruba Networks Support

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 opens.

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



Admin Login

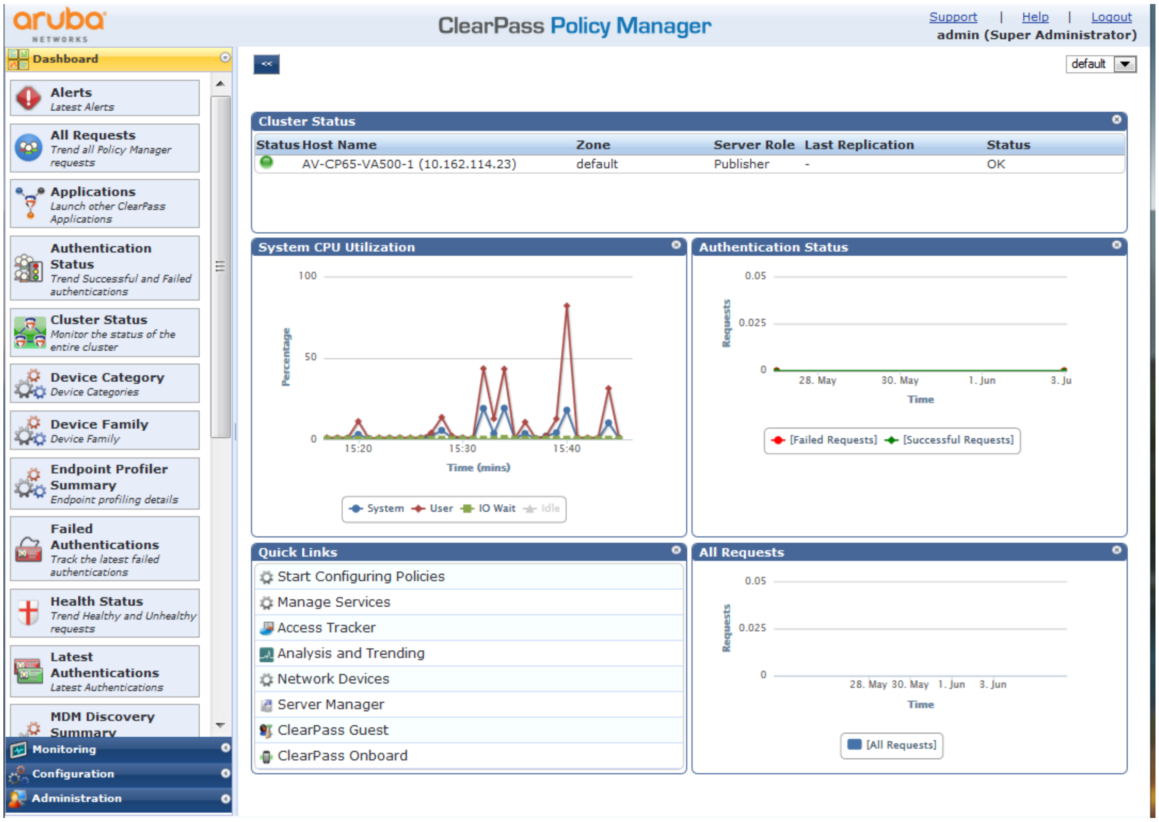
Username: admin

Password: ••••••••

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 home page is displayed.

Figure 7: *W-ClearPass Policy Manager Home Page*



Cluster Status

Status	Host Name	Zone	Server Role	Last Replication	Status
●	AV-CP65-VA500-1 (10.162.114.23)	default	Publisher	-	OK

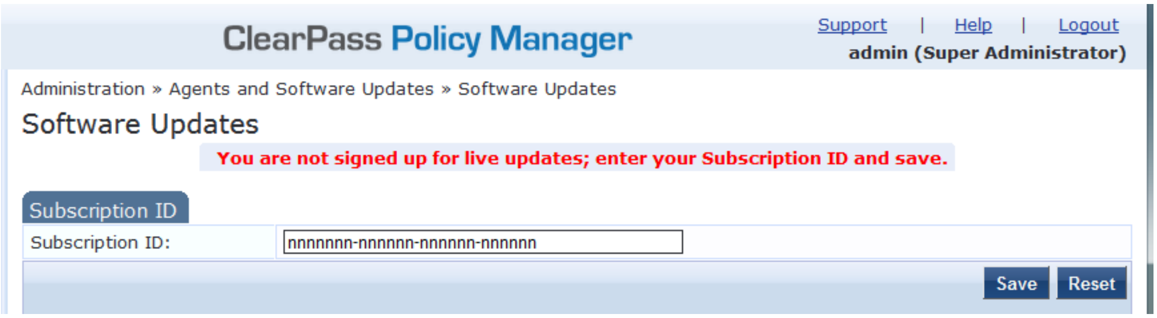
Signing Up for Live Software Updates

Upon your initial login to W-ClearPass Policy Manager, 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*



admin (Super Administrator)

Software Updates

You are not signed up for live updates; enter your Subscription ID and save.

Subscription ID: nnnnnnn-nnnnnn-nnnnnn-nnnnnn

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 displayed 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).

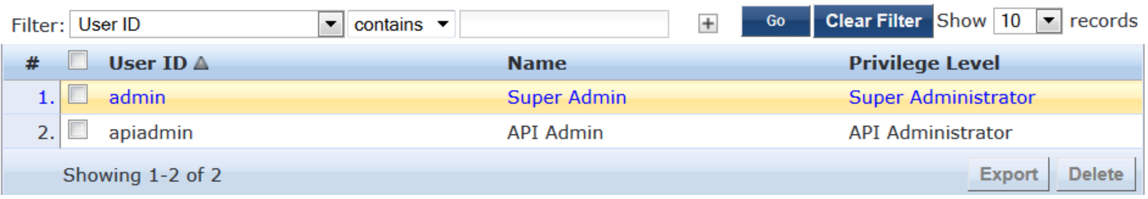
If you wish to assign a unique **admin** password, use this procedure to change it.

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*



Filter: User ID contains Show 10 records

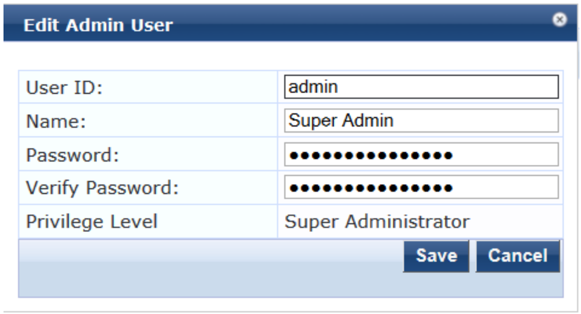
#	☐	User ID ▲	Name	Privilege Level
1.	☐	admin	Super Admin	Super Administrator
2.	☐	apiadmin	API Admin	API Administrator

Showing 1-2 of 2

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

   The **Edit Admin User** dialog 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 console using the serial port.
2. Enter the following commands:
   - `login: poweroff`
   - `password: poweroff`

The W-ClearPass hardware appliance shuts down.

NOTE

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 W-ClearPass 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 vSphere console (see Using vSphere Web Client to Install W-ClearPass on a Virtual Machine on page 21) or the Hyper-V hypervisor (Using Hyper-V to Install W-ClearPass on a Virtual Appliance on page 34).
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, open a support case with Dell Technical Support

   A unique password will be dynamically generated from the recovery key and sent 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 sent to you by Dell Technical Support.

Chapter 2
Setting Up W-ClearPass Virtual Machines

This chapter describes the procedures for using the VSphere Web Client and Hyper-V to install W-ClearPass on a virtual machine.

This chapter includes the following information:

- Using vSphere Web Client to Install W-ClearPass on a Virtual Machine
- Using Hyper-V to Install W-ClearPass on a Virtual Appliance

Using 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 ESX 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

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 W-ClearPass virtual appliance.

Supplemental Storage/Hard Disk Requirement

The 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 26 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-ClearPassI/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.

NOTE

For the latest information on the supported hypervisors and virtual hardware requirements, refer to 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 login credentials.

Supported Hypervisors

W-ClearPass supports the following ESX hypervisors:

- VMware ESX 4.0

  Recommended minimum version for CP-VA-500 and CP-VA-5K virtual appliances.

  Note that VMware ESX 4.0 does not support greater than the eight virtual CPUs required for the CP-VA-25K virtual appliance.
- 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	

Required Information	Value for Your Installation
Data port IP address (optional)	**NOTE:** Make sure that the Data interface IP address is *not* 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)	

vSphere Web Client W-ClearPass Installation Overview

W-ClearPass 6.x 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. Download the VMware ESXi package from the from the Dell Download site at http://download.dell-pcw.com/DownloadSoftware/tabid/75/Default.aspx to a folder accessible by your VMware ESXi server.
2. To extract the files, unzip the files to a folder on your server.
3. Follow the steps in the OVF wizard to deploy the OVF file, but do not power on yet.

NOTE

There is only one OVF file with all the variant types and sizes selectable when the virtual appliance boots.

4. Add a new hard disk, based on the requirements for your type of virtual machine.
5. 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. Then check the recommended virtual hardware specifications and verify that your system meets those requirements.

NOTE

W-ClearPass Release Notes are available at https://download.dell-pcw.com under the W-ClearPass 6.6.0 Upgrade folder. Access to this site requires login credentials.

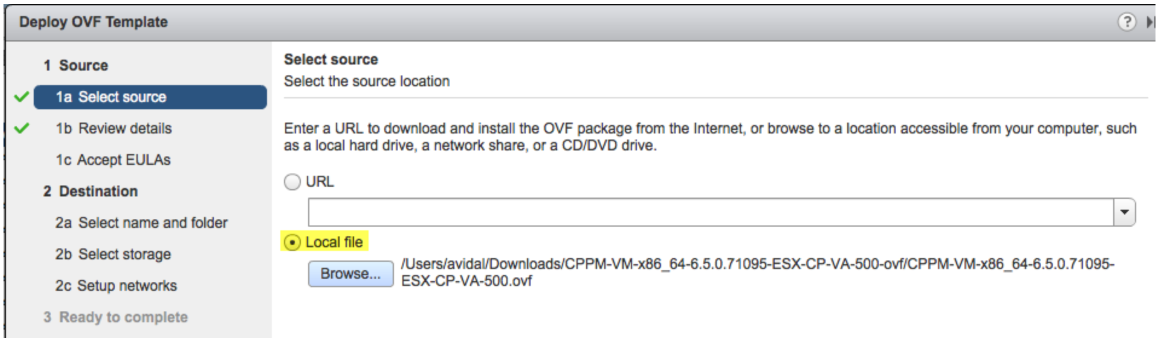
2. Start the VMware vSphere Web Client.
3. Extract the files into a folder on your desktop.
4. Using either the VMware vSphere Web Client or the standard vSphere Client, deploy the Open Virtualization Format (OVF) template that was downloaded and extracted in **Step 2** and **Step 3**.

   The Deploy OVF Template appears.

NOTE

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*



Select source

Select the source location

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

○ URL

● Local file

/Users/avidal/Downloads/CPPM-VM-x86_64-6.5.0.71095-ESX-CP-VA-500-ovf/CPPM-VM-x86_64-6.5.0.71095-ESX-CP-VA-500.ovf

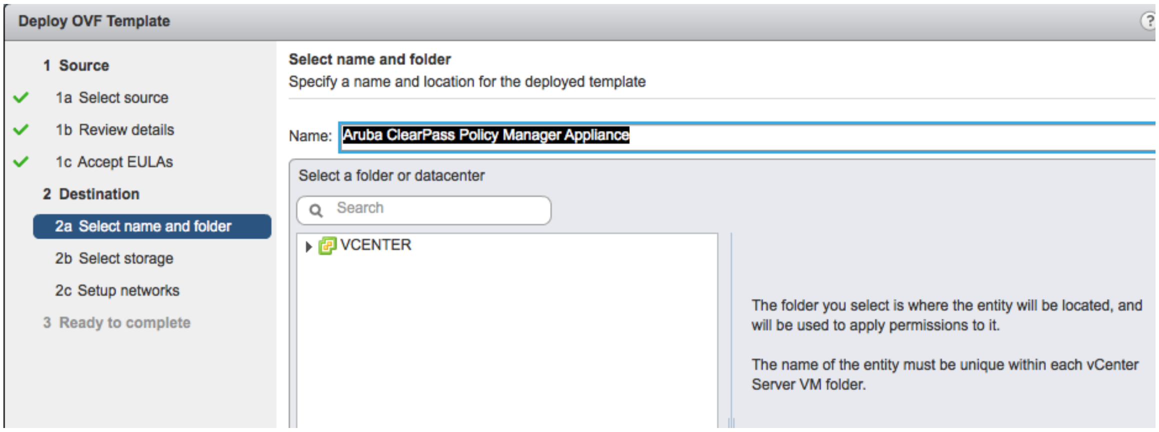
5. Select **Local File**, then click **Browse**.
6. Find the folder where you extracted the files, then click **Next**.

   The **Review Details** screen appears.
7. Review the information presented, then click **Next**.

   The **Accept EULAs** screen appears.
8. Read the End User License Agreements (EULA) and click **Accept**, then click **Next**.

   The **Select Name and Folder** screen appears.

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



Select name and folder

Specify a name and location for the deployed template

Name: Aruba ClearPass Policy Manager Appliance

Select a folder or datacenter

The folder you select is where the entity will be located, and will be used to apply permissions to it.

The name of the entity must be unique within each vCenter Server VM folder.

9. In the **Select Name and Folder** dialog:

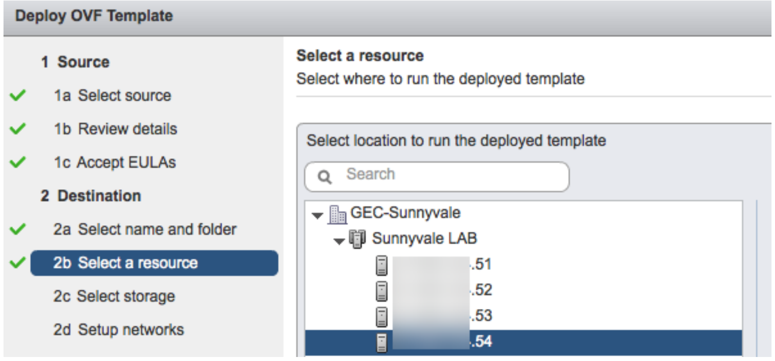
   The name of the template is set by default to *Dell W-ClearPass Policy Manager Appliance*.

   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, then click **Next**.

      The **Select a Resource** screen opens.

Figure 13: *Selecting a Resource*



Deploy OVF Template

1 Source
- ✓ 1a Select source
- ✓ 1b Review details
- ✓ 1c Accept EULAs

2 Destination
- ✓ 2a Select name and folder
- ✓ 2b Select a resource
- 2c Select storage
- 2d Setup networks

Select a resource
Select where to run the deployed template

Select location to run the deployed template

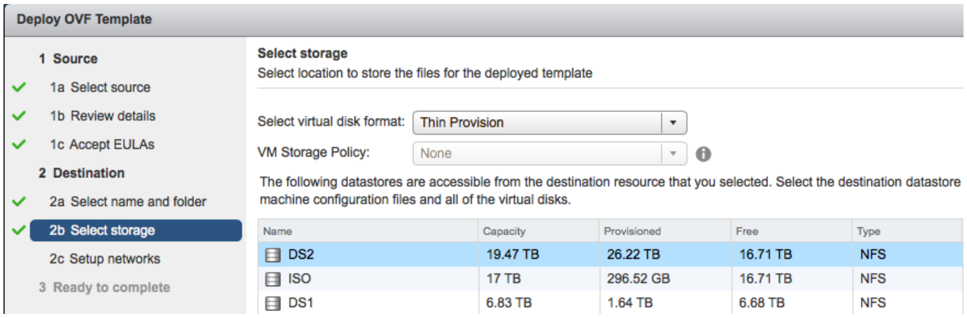
Search

- GEC-Sunnyvale
  - Sunnyvale LAB
    - [redacted].51
    - [redacted].52
    - [redacted].53
    - [redacted].54

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

    The **Select Storage** screen appears.

Figure 14: *Selecting the Location to Store the Files*



Deploy OVF Template

1 Source
- ✓ 1a Select source
- ✓ 1b Review details
- ✓ 1c Accept EULAs

2 Destination
- ✓ 2a Select name and folder
- ✓ 2b Select storage
- 2c Setup networks

3 Ready to complete

Select storage
Select location to store the files for the deployed template

Select virtual disk format: Thin Provision

VM Storage Policy: None

The following datastores are accessible from the destination resource that you selected. Select the destination datastore machine configuration files and all of the virtual disks.

Name	Capacity	Provisioned	Free	Type
DS2	19.47 TB	26.22 TB	16.71 TB	NFS
ISO	17 TB	296.52 GB	16.71 TB	NFS
DS1	6.83 TB	1.64 TB	6.68 TB	NFS

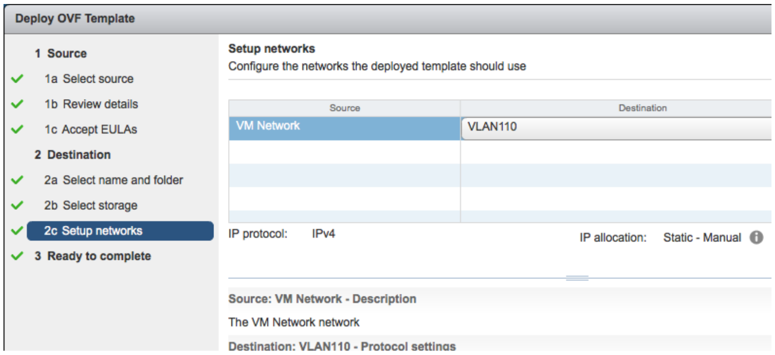
11. Choose the virtual disk format and data store for the W-ClearPass virtual appliance, then click **Next**.

NOTE

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*



Deploy OVF Template

1 Source
- ✓ 1a Select source
- ✓ 1b Review details
- ✓ 1c Accept EULAs

2 Destination
- ✓ 2a Select name and folder
- ✓ 2b Select storage
- ✓ 2c Setup networks

✓ 3 Ready to complete

Setup networks
Configure the networks the deployed template should use

Source	Destination
VM Network	VLAN110

IP protocol: IPv4

IP allocation: Static - Manual

Source: VM Network - Description
The VM Network network
Destination: VLAN110 - Protocol settings

12. Specify the virtual network where W-ClearPass will reside, then click **Next**.

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

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

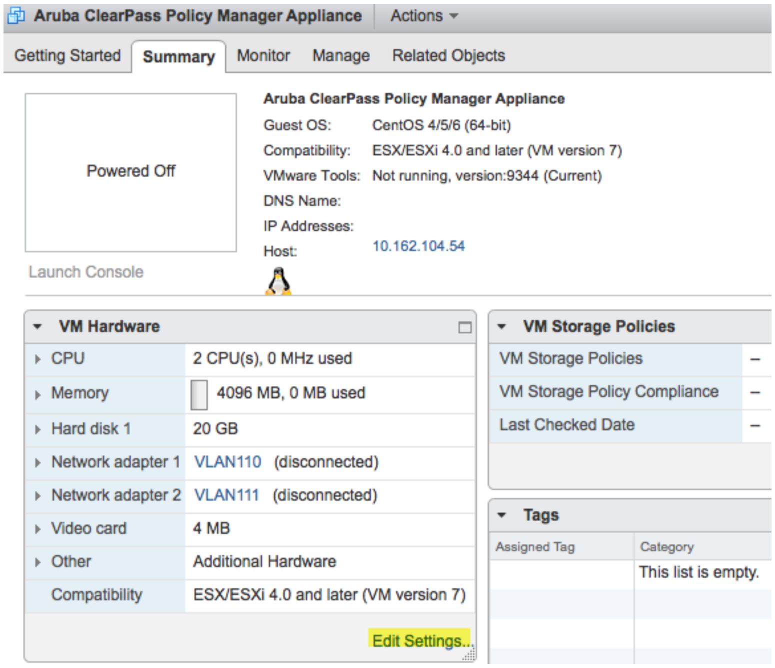
    The OVF is deployed in the selected network.

Adding a Virtual Hard Disk

After the OVF 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*



Aruba ClearPass Policy Manager Appliance

Guest OS: CentOS 4/5/6 (64-bit)
Compatibility: ESX/ESXi 4.0 and later (VM version 7)
VMware Tools: Not running, version:9344 (Current)
DNS Name:
IP Addresses:
Host: 10.162.104.54

VM Hardware	
CPU	2 CPU(s), 0 MHz used
Memory	4096 MB, 0 MB used
Hard disk 1	20 GB
Network adapter 1	VLAN110 (disconnected)
Network adapter 2	VLAN111 (disconnected)
Video card	4 MB
Other	Additional Hardware
Compatibility	ESX/ESXi 4.0 and later (VM version 7)

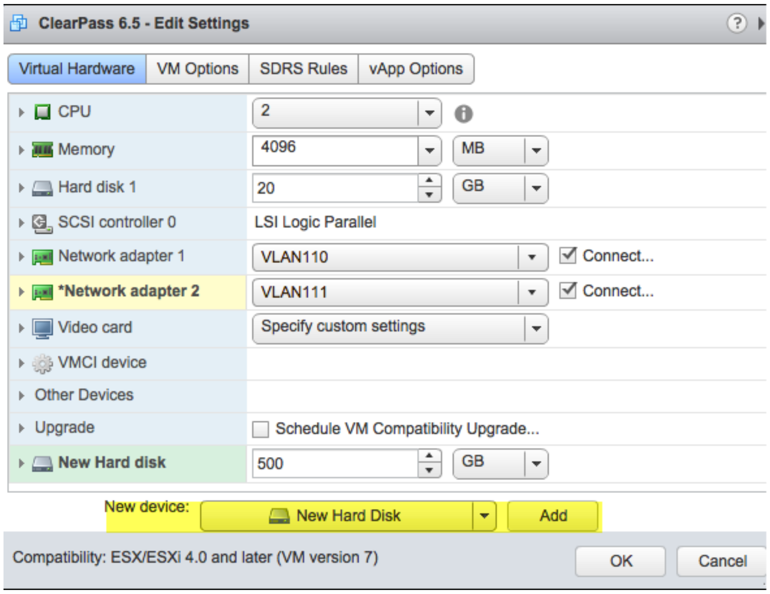
VM Storage Policies	
VM Storage Policies	–
VM Storage Policy Compliance	–
Last Checked Date	–

Assigned Tag	Category
	This list is empty.

2. Click **Edit Settings**.

   The **Edit Settings** dialog appears.

Figure 17: *Editing the Virtual Machine Settings*



ClearPass 6.5 - Edit Settings

Virtual Hardware	
CPU	2
Memory	4096 MB
Hard disk 1	20 GB
SCSI controller 0	LSI Logic Parallel
Network adapter 1	VLAN110 ☑ Connect...
*Network adapter 2	VLAN111 ☑ Connect...
Video card	Specify custom settings
VMCI device	
Other Devices	
Upgrade	□ Schedule VM Compatibility Upgrade...
New Hard disk	500 GB

New device: New Hard Disk

Compatibility: ESX/ESXi 4.0 and later (VM version 7)

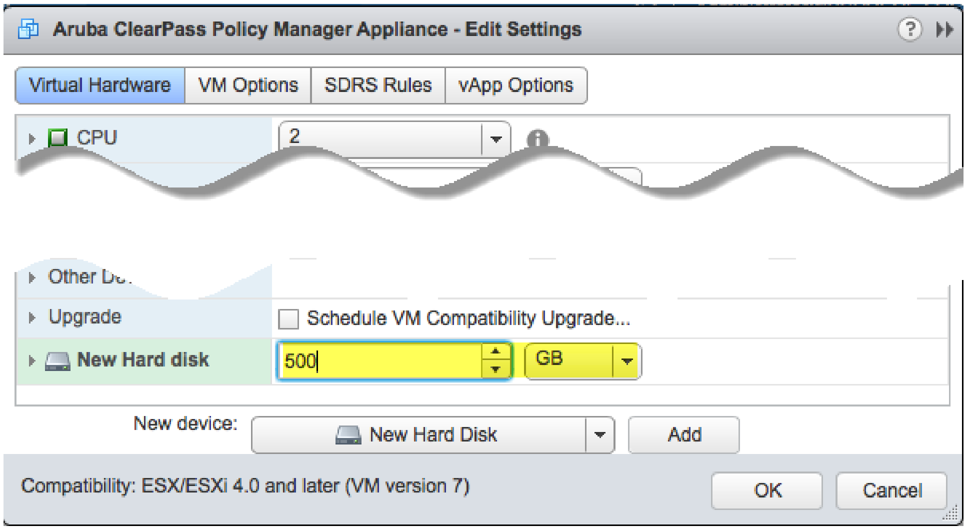
3. Add a new virtual hard disk:

   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**.

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



CPU: 2

□ Schedule VM Compatibility Upgrade...

New Hard disk: 500 GB

New device: New Hard Disk

Compatibility: ESX/ESXi 4.0 and later (VM version 7)

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

> NOTE
>
> 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 6.6.0 Upgrade folder. Access to this site requires login credentials.

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

   a. **Network adapter 1**: Assigned to the **Management port**.

   b. **Network adapter 2**: Assigned to the **Data port**.

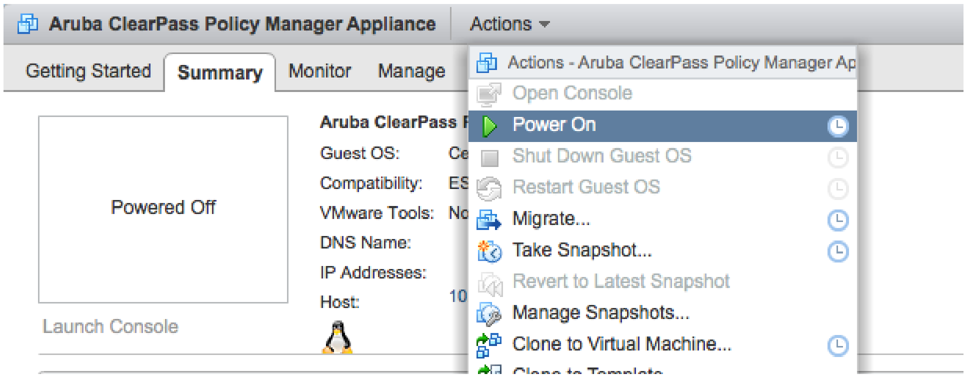
   c. Click **OK**.

Launching the W-ClearPass Virtual Appliance

To launch the Dell W-ClearPass Policy Manager virtual appliance:

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

Figure 19: *Powering on the Virtual Appliance*

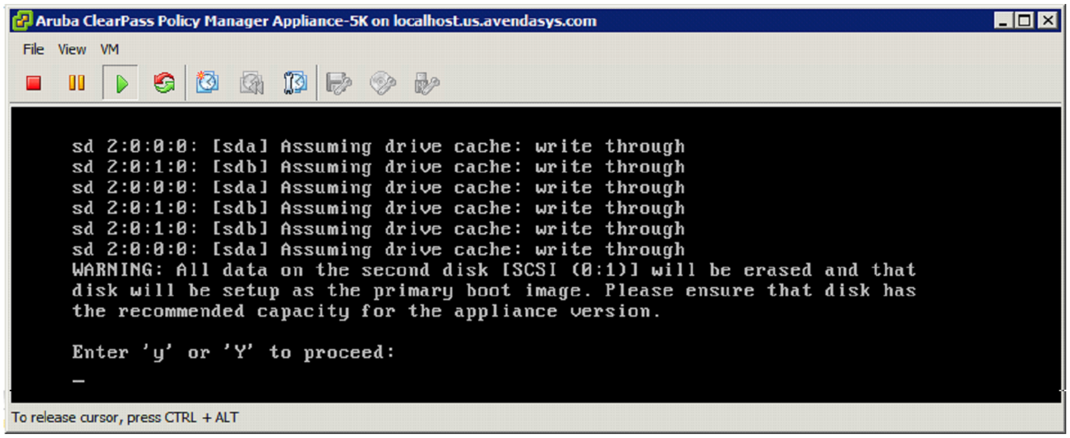


The virtual appliance is now powered on.

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

   The initial VM console screen is displayed.

Figure 20: *Initial Virtual Machine Console Screen*


Aruba ClearPass Policy Manager Appliance-5K on localhost.us.avendasys.com
File
View
VM
To release cursor, press CTRL + ALT

```
sd 2:0:0:0: [sda] Assuming drive cache: write through
sd 2:0:1:0: [sdb] Assuming drive cache: write through
sd 2:0:0:0: [sda] Assuming drive cache: write through
sd 2:0:1:0: [sdb] Assuming drive cache: write through
sd 2:0:1:0: [sdb] Assuming drive cache: write through
sd 2:0:0:0: [sda] Assuming drive cache: write through
WARNING: All data on the second disk [SCSI (0:1)] will be erased and that
disk will be setup as the primary boot image. Please ensure that disk has
the recommended capacity for the appliance version.

Enter 'y' or 'Y' to proceed:
_
```

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.

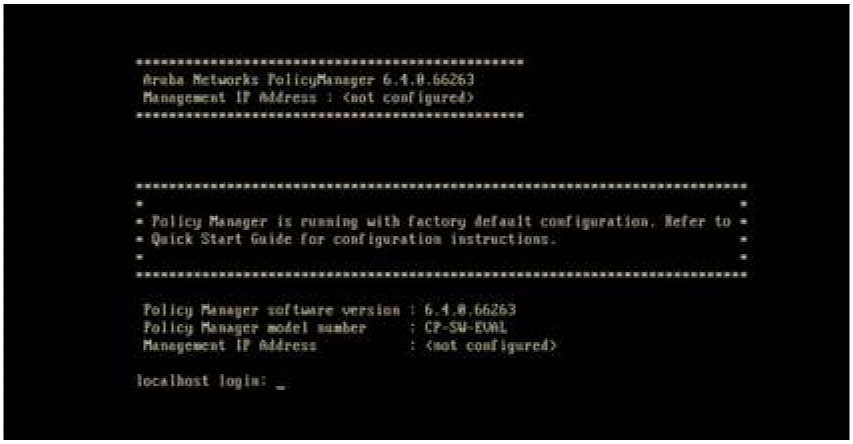
   When the rebooting process is complete, the W-ClearPass virtual appliance is configured, and the virtual appliance will power on and boot up within a couple of minutes.

NOTE

The whole process, from deploying the OVF image to the presentation of the login banner screen, typically takes between 30 and 40 minutes.

4. After the W-ClearPass virtual appliance launches correctly, the following banner is displayed:

Figure 21: *Virtual Machine Login Banner*



```
***********************************************
 Aruba Networks PolicyManager 6.4.0.66263
 Management IP Address : <not configured>
***********************************************



**************************************************************************
*                                                                        *
* Policy Manager is running with factory default configuration. Refer to *
* Quick Start Guide for configuration instructions.                      *
*                                                                        *
**************************************************************************

 Policy Manager software version : 6.4.0.66263
 Policy Manager model number     : CP-SW-EVAL
 Management IP Address           : <not configured>

localhost login: _
```

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 W-ClearPass 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**.

NOTE

> 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 33.

   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

NOTE

> 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:

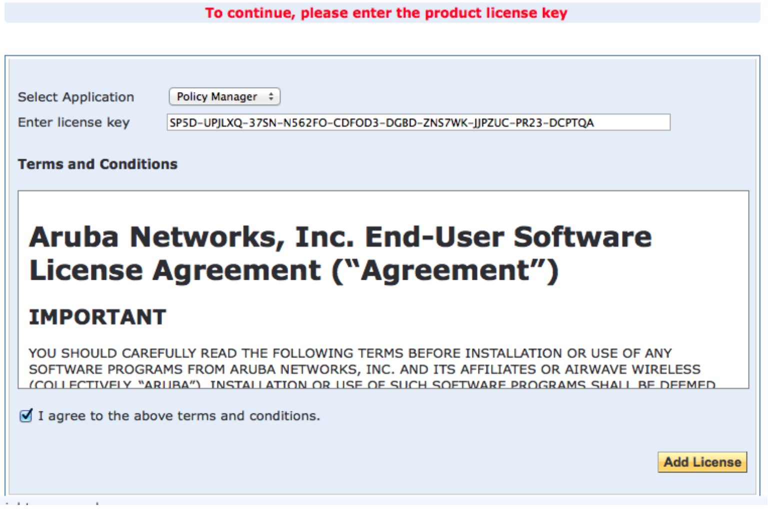
1. After the configuration has been applied at the virtual appliance console, open a web browser and go to the W-ClearPass management interface:

   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 22: *Entering the License Key*



To continue, please enter the product license key

Select Application: Policy Manager

Enter license key: SP5D-UPJLXQ-37SN-N562FO-CDFOD3-DGBD-ZNS7WK-JJPZUC-PR23-DCPTQA

Terms and Conditions

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

IMPORTANT

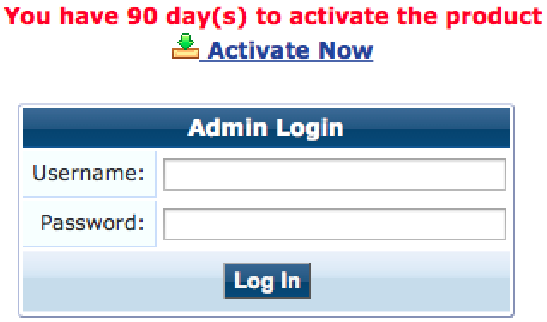
YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY “ARUBA”). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED

☑ I agree to the above terms and conditions.

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 23: *Activating W-ClearPass*



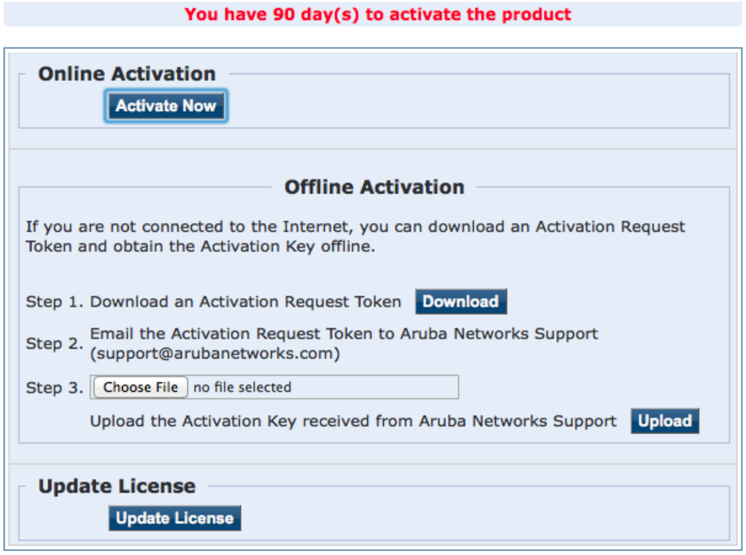
You have 90 day(s) to activate the product

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

   When you click **Activate Now**, W-ClearPass Policy Manager attempts to activate the license over the Internet with Dell 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 24.

Figure 24: *Performing Offline Activation*



You have 90 day(s) to activate the product

Offline Activation

If you are not connected to the Internet, you can download an Activation Request Token and obtain the Activation Key offline.

Step 1. Download an Activation Request Token

Step 2. Email the Activation Request Token to Aruba Networks Support (support@arubanetworks.com)

Step 3. no file selected

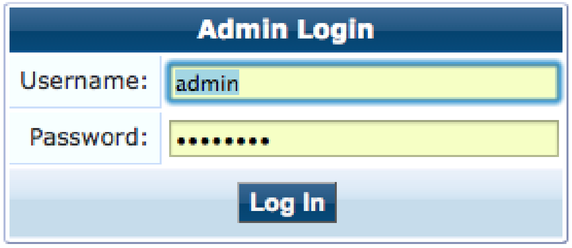
Upload the Activation Key received from Aruba Networks Support

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 25: *Logging in to the W-ClearPass Virtual Appliance*



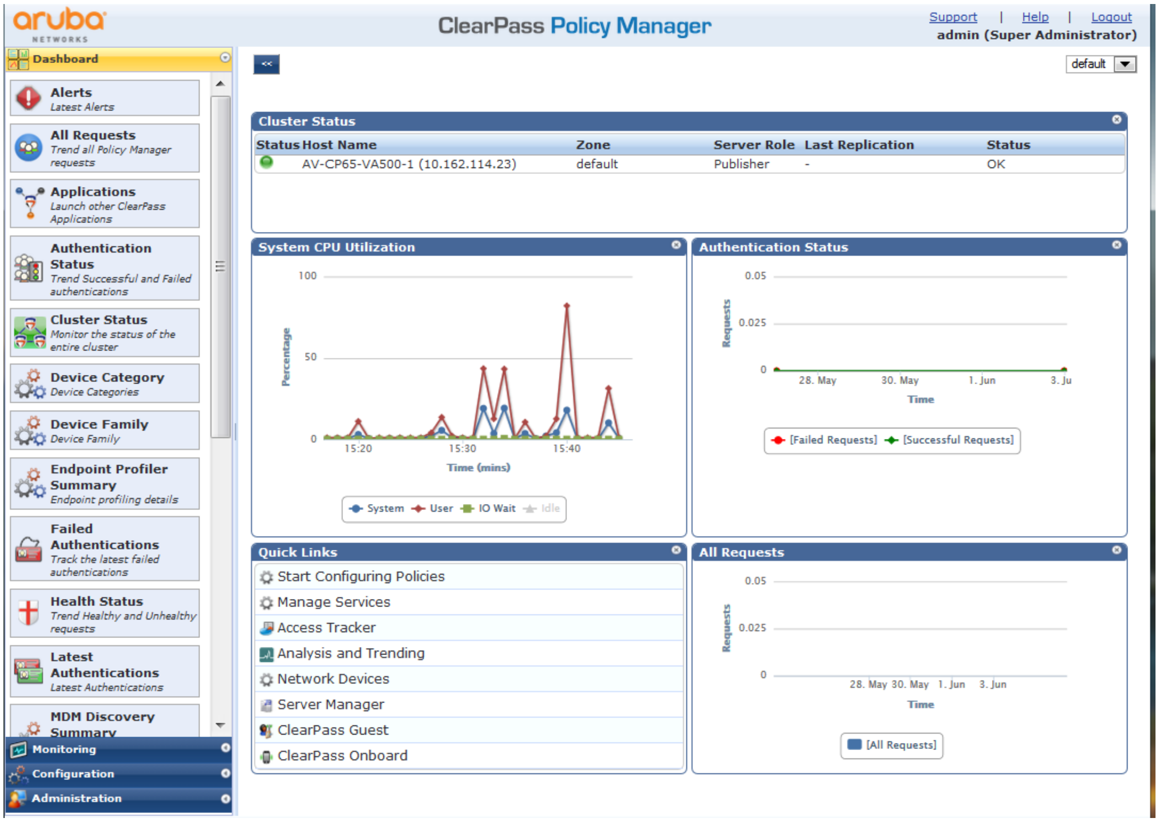
Username: admin

Password: ••••••••

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 28.
2. Click **Log In**.

   The W-ClearPass Policy Manager Home Page opens.

Figure 26: *W-ClearPass Policy Manager Home Page*



Status	Host Name	Zone	Server Role	Last Replication	Status
●	AV-CP65-VA500-1 (10.162.114.23)	default	Publisher	-	OK

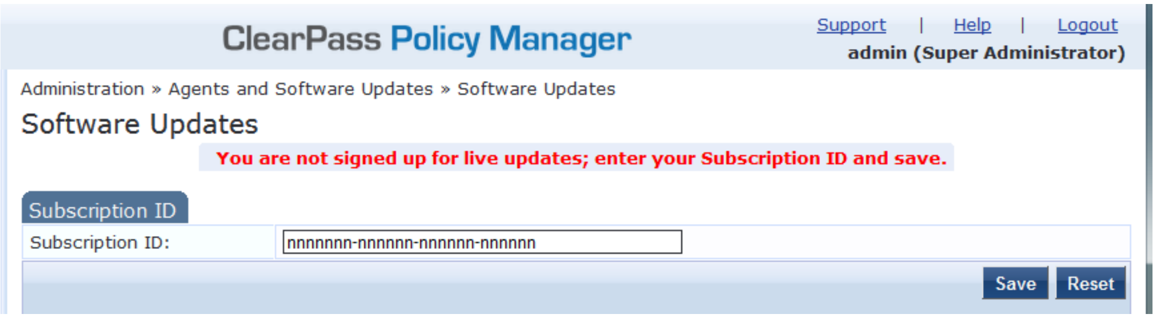
Signing Up for Live Software Updates

Upon your initial login to W-ClearPass Policy Manager, Dell recommends that you 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 27: *Entering the Subscription ID for Live Updates*


ClearPass Policy Manager
Support | Help | Logout
admin (Super Administrator)
Administration » Agents and Software Updates » Software Updates
Software Updates
Subscription ID
Save
Reset

You are not signed up for live updates; enter your Subscription ID and save.

Subscription ID: nnnnnnn-nnnnnn-nnnnnn-nnnnnn

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

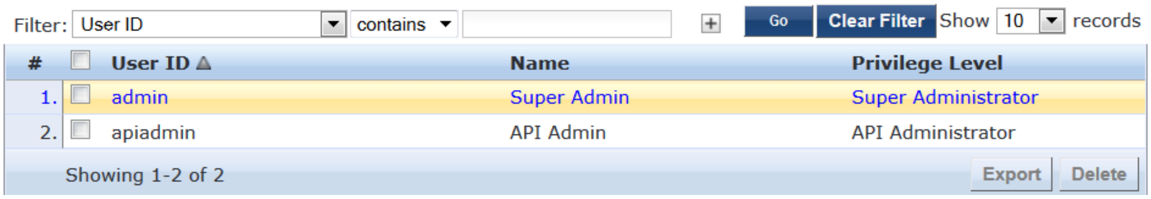
When the cluster password for this W-ClearPass server is set upon initial configuration (see Completing the Virtual Appliance Setup on page 28), the administration password is also set to the same password. If you wish to assign a unique **admin** password, use this procedure to change it.

To change the administration password:

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

   The **Admin Users** page opens.

Figure 28: *Admin Users Page*



Filter: User ID contains

Show 10 records

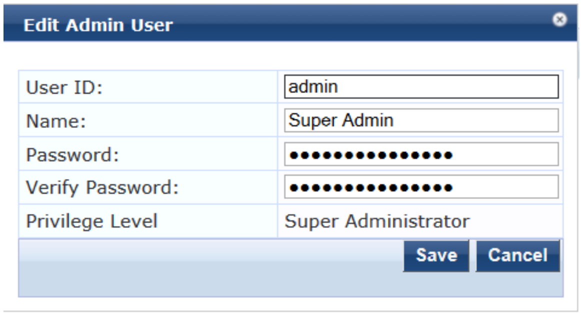
#	□	User ID △	Name	Privilege Level
1.	□	admin	Super Admin	Super Administrator
2.	□	apiadmin	API Admin	API Administrator

Showing 1-2 of 2

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

   The **Edit Admin User** dialog opens.

Figure 29: *Changing the Administration Password*



Edit Admin User

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. 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 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 hypvervisor, 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.

> NOTE
>
> This section assumes that the 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 Hyper-V Hypervisors

W-ClearPass Policy Manager supports the following Hyper-V hypervisors:

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

> NOTE
>
> For the latest information on the supported hypervisors and virtual hardware requirements, refer to 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 login credentials.

Meeting the Recommended Hyper-V Server Specifications

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 don't have the virtual appliance resources to support a full workload, consider ordering the W-ClearPass Policy Manager hardware appliance.

Supplemental Storage/Hard Disk Requirement

The W-ClearPass Hyper-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 39 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-ClearPassI/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 *not* 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)	

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. From the Dell Support Center (https://download.dell-pcw.com), download the Hyper-V package and copy the files to a folder on your server.
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.

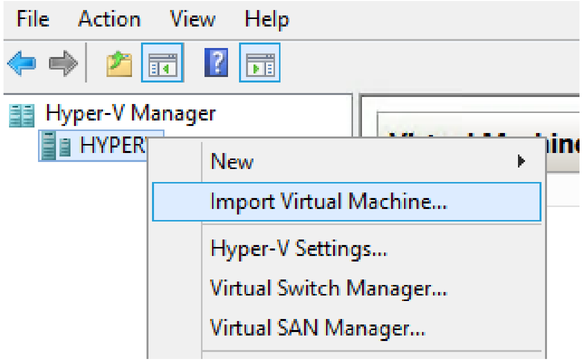
Importing the Virtual Machine

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

To import the virtual appliance:

1. Download the Hyper-V package from the from the Dell Download site at http://download.dell-pcw.com/DownloadSoftware/tabid/75/Default.aspx to a folder accessible by your 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** (see Figure 30).

Figure 30: *Selecting the "Import Virtual Machine" Option*

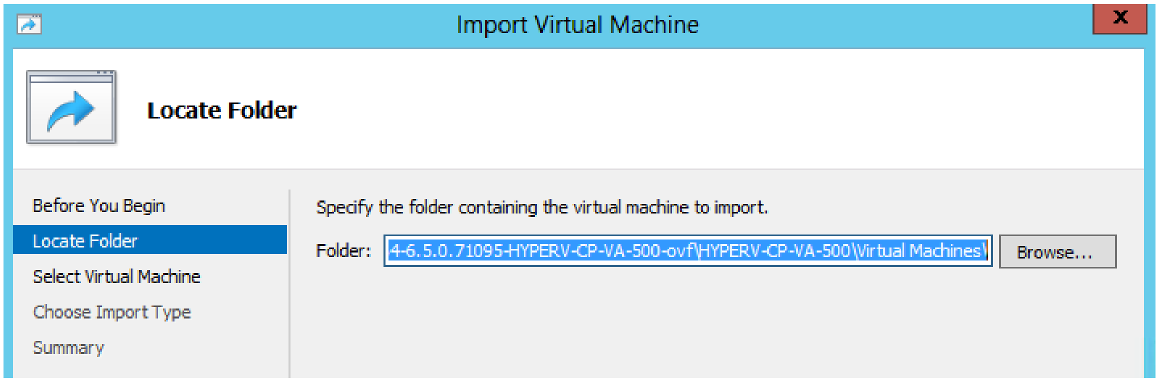


The **Before You Begin** dialog opens.

5. Click **Next**.

   The **Locate Folder** dialog opens.

Figure 31: *Locating the Folder*



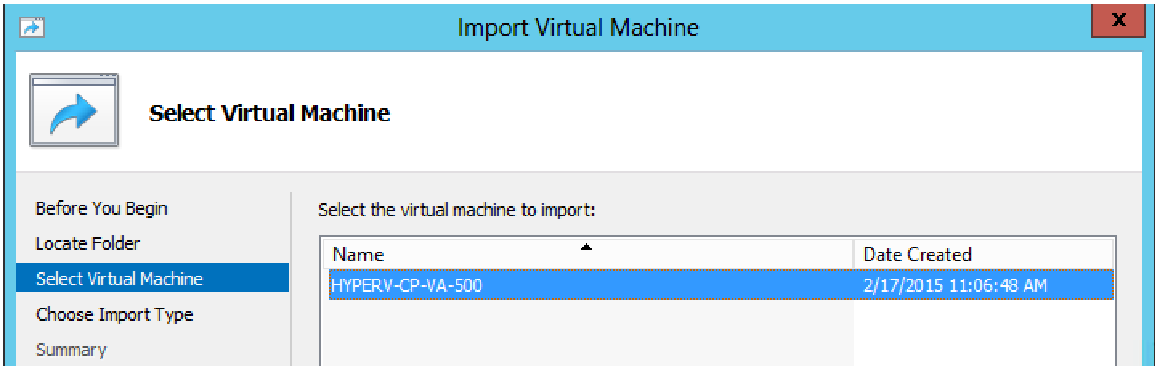
Specify the folder containing the virtual machine to import.

Folder: 4-6.5.0.71095-HYPERV-CP-VA-500-ovf\HYPERV-CP-VA-500\Virtual Machines\

6. In the **Locate Folder** step, select the folder you unzipped in **Step 1**, then click **Next**.

   The **Select Virtual Machine** dialog opens.

Figure 32: *Selecting the Virtual Machine*



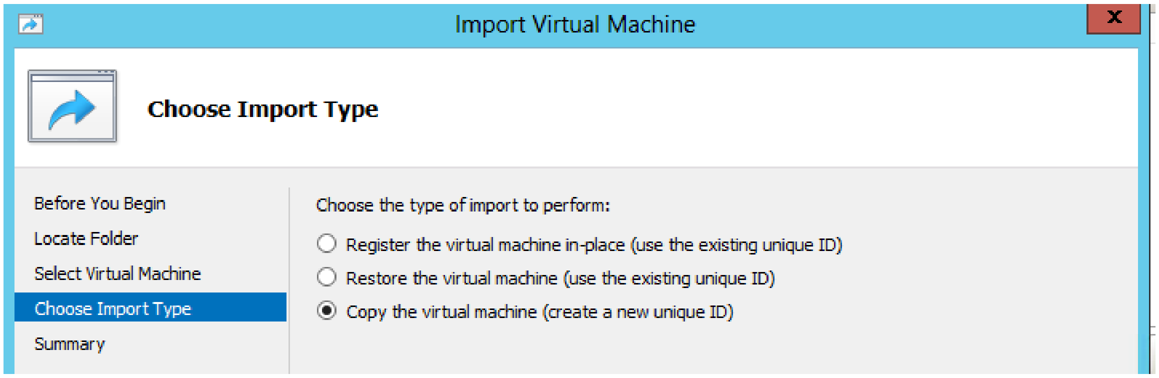
Select the virtual machine to import:

Name	Date Created
HYPERV-CP-VA-500	2/17/2015 11:06:48 AM

7. Make sure the correct virtual appliance is highlighted, then click **Next**.

   The **Choose Import Type** dialog opens.

Figure 33: *Specifying the Import Type*



Choose the type of import to perform:

○ Register the virtual machine in-place (use the existing unique ID)

○ Restore the virtual machine (use the existing unique ID)

● Copy the virtual machine (create a new unique ID)

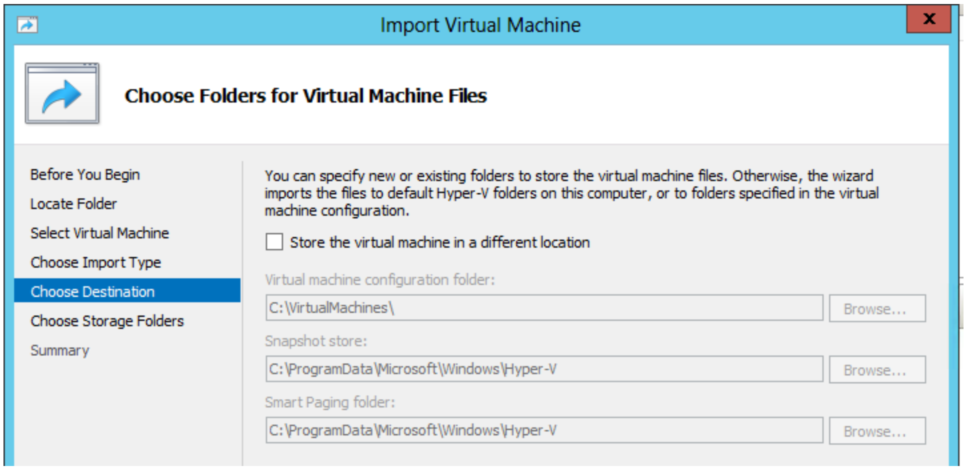
8. In the **Choose Import Type** step, select **Copy the virtual machine**, then click **Next**.

NOTE

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 34: *Specifying the Folders for the Virtual Machine Files*



You can specify new or existing folders to store the virtual machine files. Otherwise, the wizard imports the files to default Hyper-V folders on this computer, or to folders specified in the virtual machine configuration.

☐ Store the virtual machine in a different location

Virtual machine configuration folder: C:\VirtualMachines\

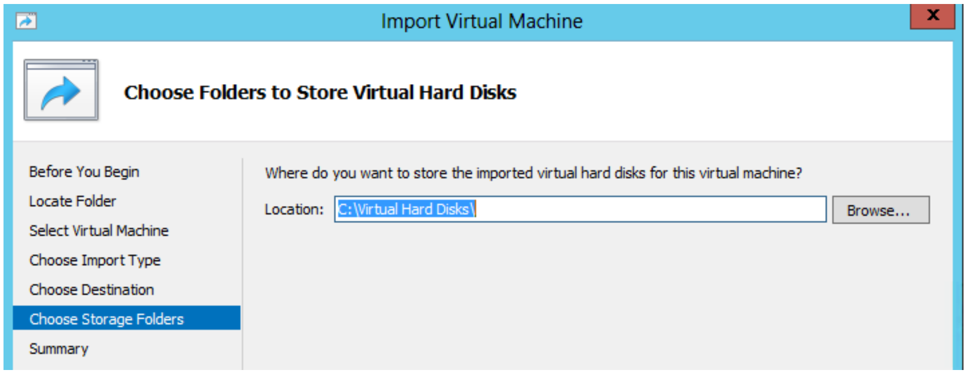
Snapshot store: C:\ProgramData\Microsoft\Windows\Hyper-V

Smart Paging folder: C:\ProgramData\Microsoft\Windows\Hyper-V

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 35: *Specifying Folders to Store Virtual Hard Disks*



Where do you want to store the imported virtual hard disks for this virtual machine?

Location: C:\Virtual Hard Disks\

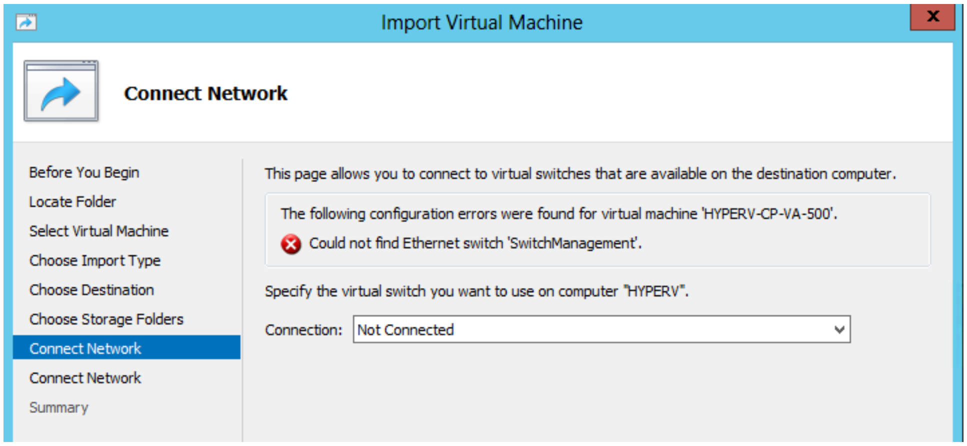
10. Accept the default virtual hard drive storage folder, or browse to a new location to change it to your preferred location, then click **Next**.

NOTE

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 36: *Specifying the Virtual Switch in the Event of an Error*


Import Virtual Machine

Connect Network

This page allows you to connect to virtual switches that are available on the destination computer.

The following configuration errors were found for virtual machine 'HYPERV-CP-VA-500'.

Could not find Ethernet switch 'SwitchManagement'.

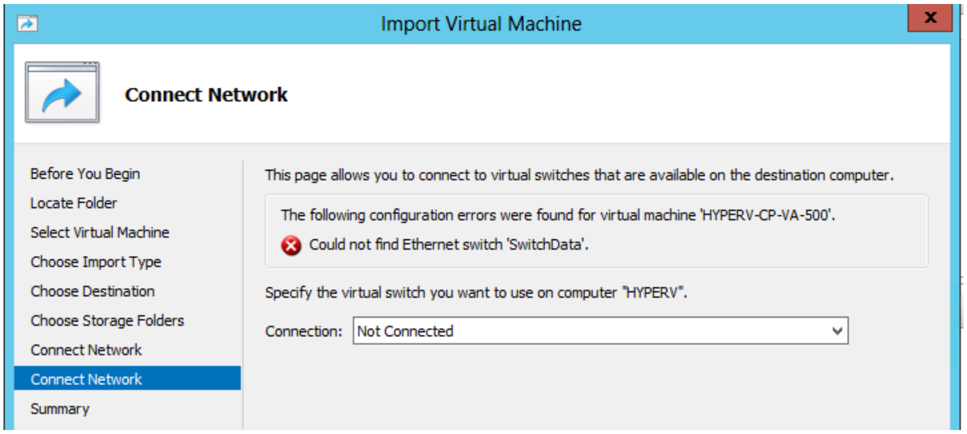
Specify the virtual switch you want to use on computer "HYPERV".

Connection: Not Connected

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 Connect Network dialog will be displayed to allow you to (optionally) specify the Data interface of the W-ClearPass Policy Manager virtual appliance.

Figure 37: *Specifying the Data Interface (Optional)*


Import Virtual Machine

Connect Network

This page allows you to connect to virtual switches that are available on the destination computer.

The following configuration errors were found for virtual machine 'HYPERV-CP-VA-500'.

Could not find Ethernet switch 'SwitchData'.

Specify the virtual switch you want to use on computer "HYPERV".

Connection: Not Connected

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

NOTE

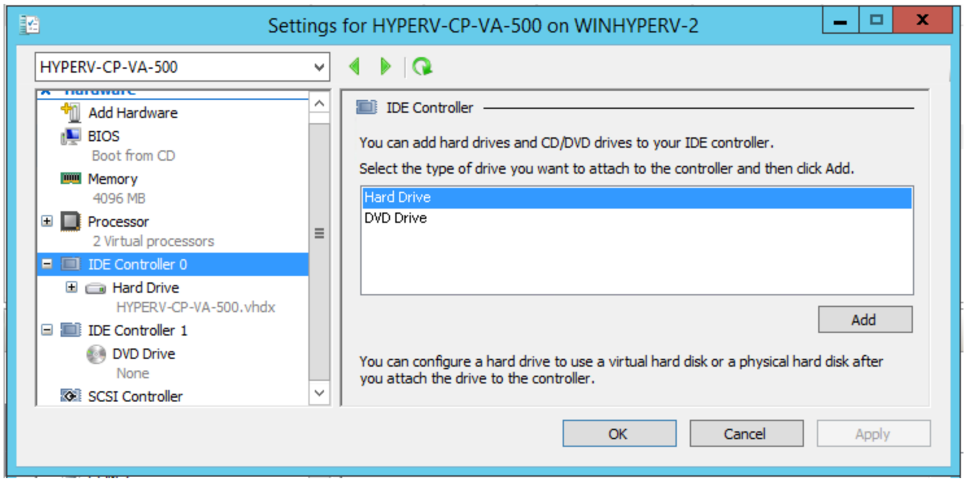
Do not create the virtual hard disk in a folder that is marked for encryption. Virtual hard disks are stored as .vhd files. Hyper-V does not support the use of storage media if Encrypting File System (EFS) has been used to encrypt the .vhd file. However, you can use files stored on a volume that uses 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 38: *Specifying the Controller*



Settings for HYPERV-CP-VA-500 on WINHYPERV-2

HYPERV-CP-VA-500

IDE Controller

You can add hard drives and CD/DVD drives to your IDE controller.

Select the type of drive you want to attach to the controller and then click Add.

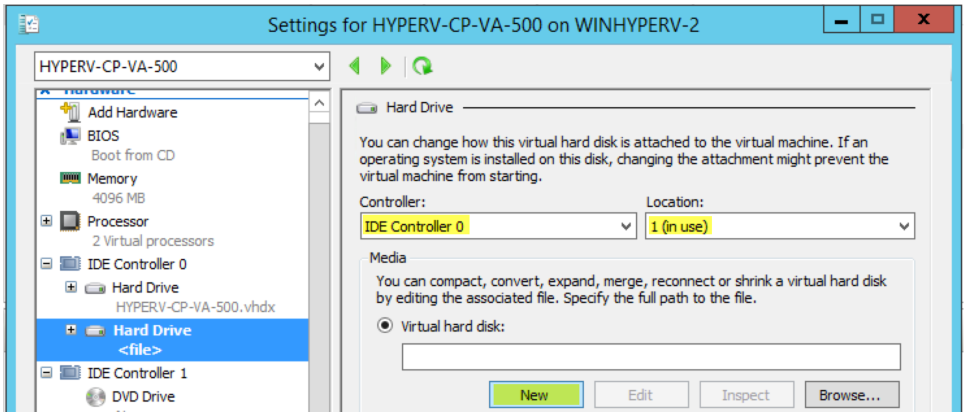
Hard Drive
DVD Drive

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to 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 39: *Configuring the Hard Drive*



Settings for HYPERV-CP-VA-500 on WINHYPERV-2

HYPERV-CP-VA-500

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 1 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

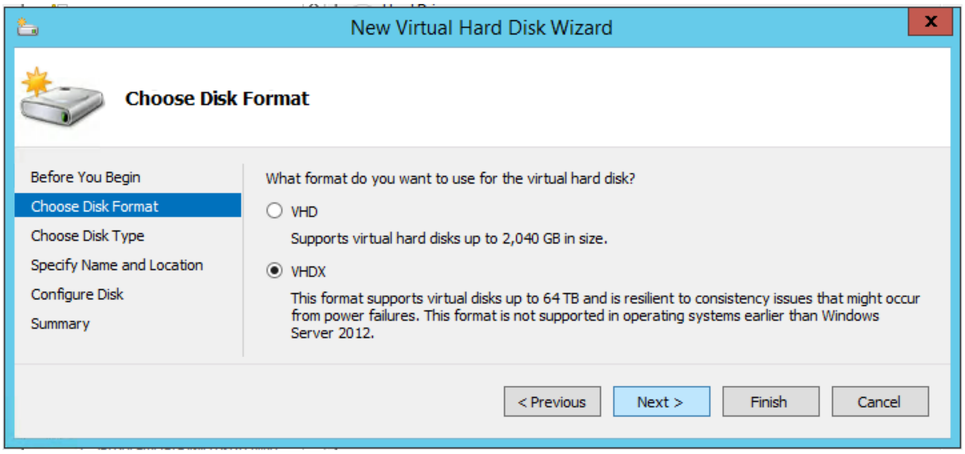
● Virtual hard disk:

5. In the **Hard Drive** dialog:
   a. **Controller**: Set to **IDE Controller 0**.
   b. **Location**: Set to **1 (in use)**.
6. Below the **Virtual hard disk** field, click **New**.

   The **New Virtual Hard Disk Wizard** opens.
7. From the **Before You Begin** dialog, click **Next**.

   The **Choose Disk Format** dialog opens.

Figure 40: *Specifying the Disk Format*



New Virtual Hard Disk Wizard

Choose Disk Format

What format do you want to use for the virtual hard disk?

○ VHD

Supports virtual hard disks up to 2,040 GB in size.

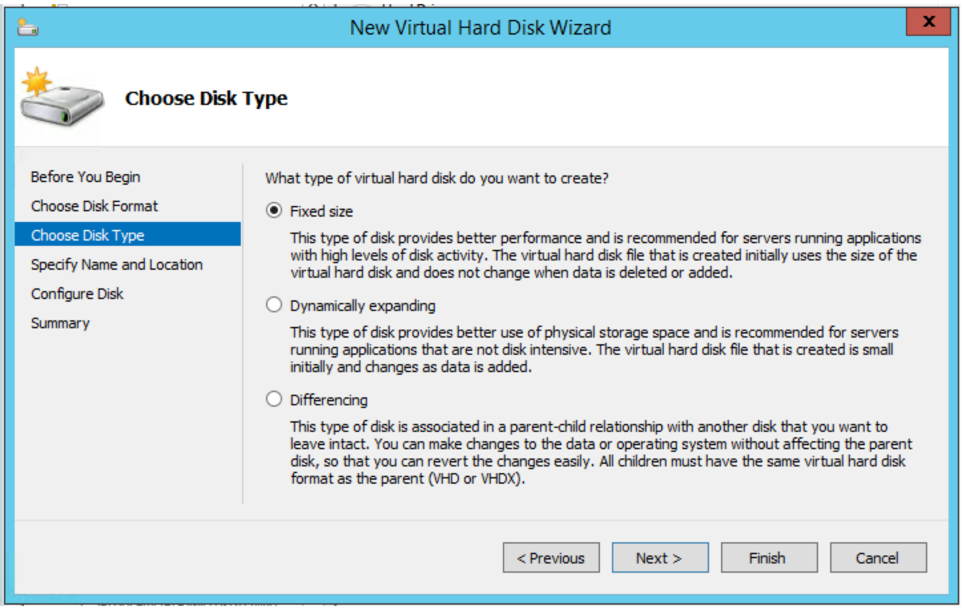
● VHDX

This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012.

8. For the disk format, choose **VHDX**, then click **Next**.

   The **Choose Disk Type** dialog opens.

Figure 41: *Specifying the Virtual Hard Disk Type*



New Virtual Hard Disk Wizard

Choose Disk Type

What type of virtual hard disk do you want to create?

● Fixed size

This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.

○ Dynamically expanding

This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added.

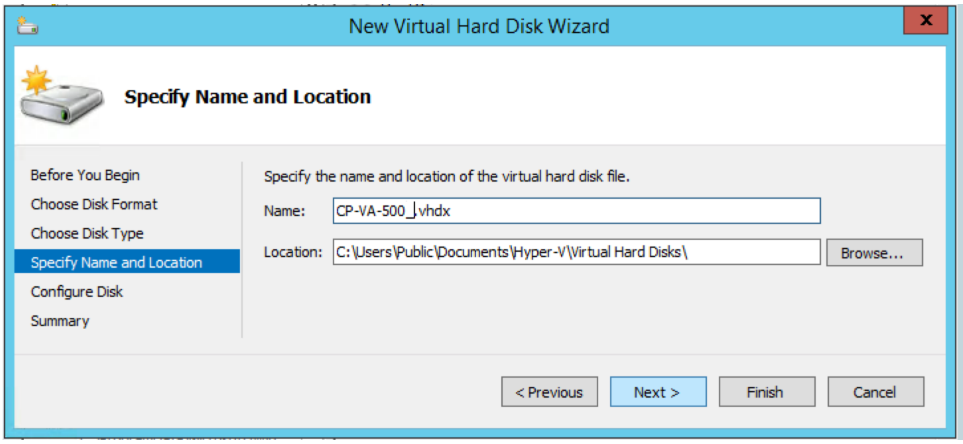
○ Differencing

This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

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

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

Figure 42: *Specifying the Name and Location of the Hard Disk File*



Specify the name and location of the virtual hard disk file.

Name: CP-VA-500_.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

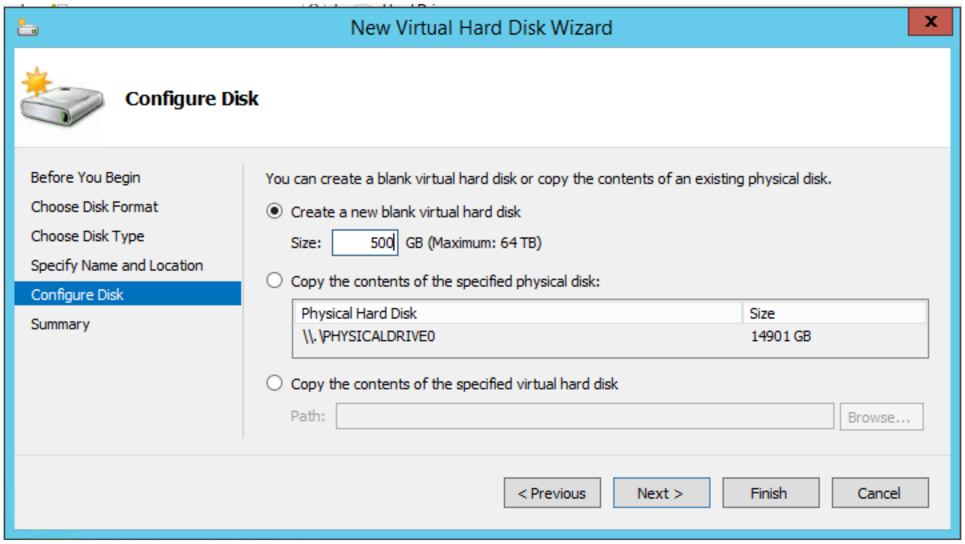
10. Do the following:

    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 43: *Configuring the New Virtual Hard Disk*



You can create a blank virtual hard disk or copy the contents of an existing physical disk.

● Create a new blank virtual hard disk

Size: 500 GB (Maximum: 64 TB)

○ Copy the contents of the specified physical disk:

Physical Hard Disk	Size
\\.\PHYSICALDRIVE0	14901 GB

○ Copy the contents of the specified virtual hard disk

Path:

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

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

       The recommended virtual hard disk size depends on the number of unique endpoints that will be supported:

       - EVAL: **80 GB**
       - 500 endpoints: **500 GB**
       - 5,000 endpoints: **1000 GB**
       - 25,000 endpoints: **1800 GB**

NOTE

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 6.6.0 Upgrade folder. Access to this site requires login credentials.

b. When finished, click **Next**.

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

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

NOTE

Depending on the options you choose for the virtual hard disk, the process can take a considerable amount of time.

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:

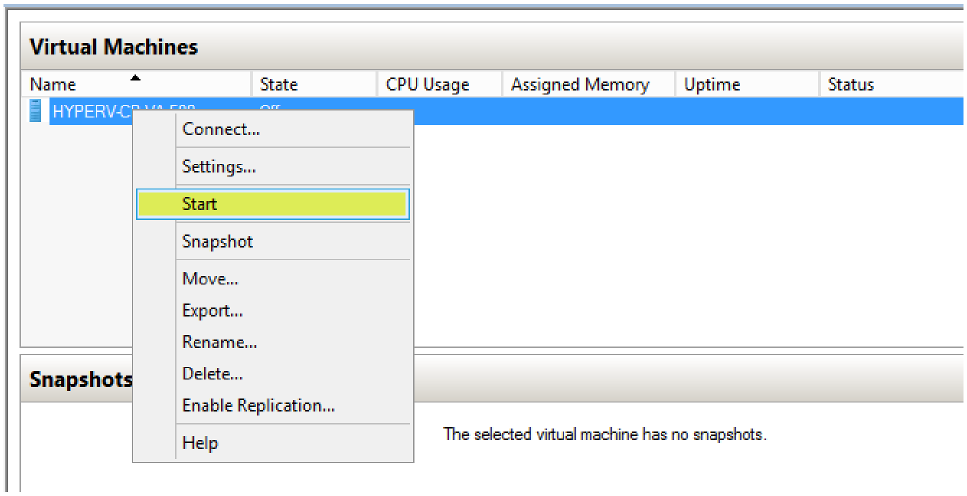
- By default, membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. However, an administrator can use Authorization Manager to modify the authorization policy so that a user or group of users can complete this procedure.
- Virtual hard disks are stored as .vhd files, which makes them portable, but it also poses a potential security risk. Dell recommends that you mitigate this risk by taking precautions such as storing the .vhd files in a secure location.
- 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 start the Dell W-ClearPass Policy Manager virtual appliance:

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

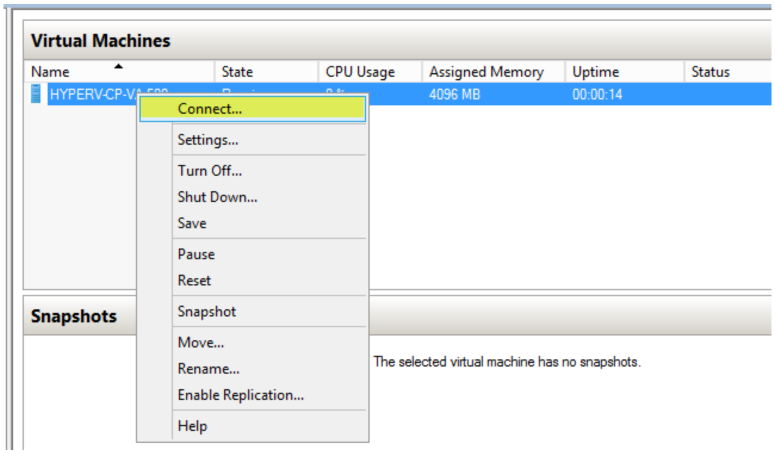
Figure 44: *Starting the Virtual Appliance*



The virtual appliance powers on.

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

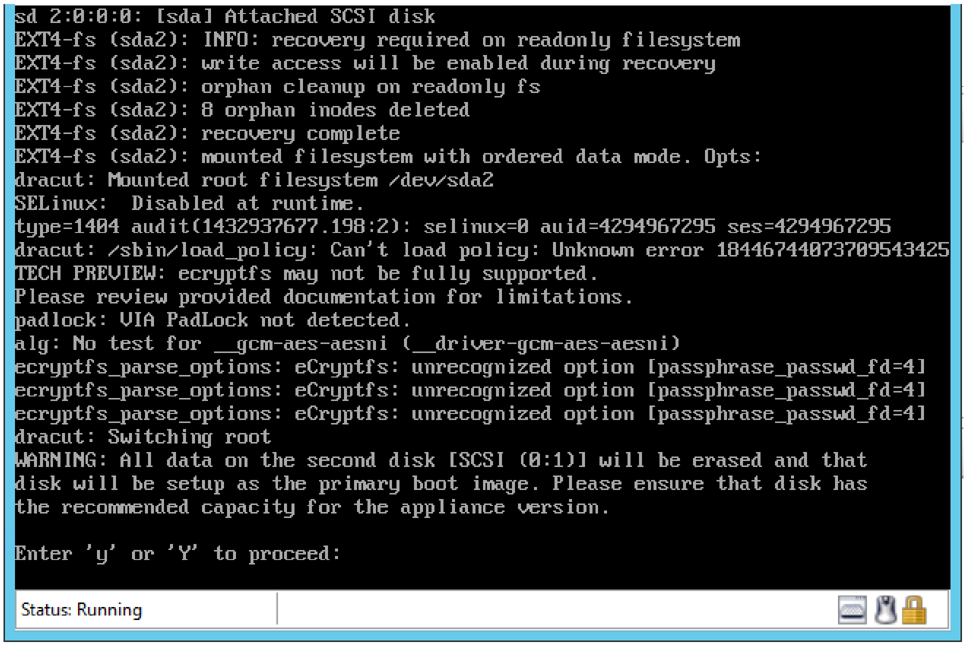
Figure 45: *Launching the VM Console*



The selected virtual machine has no snapshots.

The initial virtual machine console screen is displayed.

Figure 46: *Initial Virtual Machine Console Screen*



```
sd 2:0:0:0: [sda] Attached SCSI disk
EXT4-fs (sda2): INFO: recovery required on readonly filesystem
EXT4-fs (sda2): write access will be enabled during recovery
EXT4-fs (sda2): orphan cleanup on readonly fs
EXT4-fs (sda2): 8 orphan inodes deleted
EXT4-fs (sda2): recovery complete
EXT4-fs (sda2): mounted filesystem with ordered data mode. Opts:
dracut: Mounted root filesystem /dev/sda2
SELinux:  Disabled at runtime.
type=1404 audit(1432937677.198:2): selinux=0 auid=4294967295 ses=4294967295
dracut: /sbin/load_policy: Can't load policy: Unknown error 18446744073709543425
TECH PREVIEW: ecryptfs may not be fully supported.
Please review provided documentation for limitations.
padlock: VIA PadLock not detected.
alg: No test for __gcm-aes-aesni (__driver-gcm-aes-aesni)
ecryptfs_parse_options: eCryptfs: unrecognized option [passphrase_passwd_fd=4]
ecryptfs_parse_options: eCryptfs: unrecognized option [passphrase_passwd_fd=4]
ecryptfs_parse_options: eCryptfs: unrecognized option [passphrase_passwd_fd=4]
dracut: Switching root
WARNING: All data on the second disk [SCSI (0:1)] will be erased and that
disk will be setup as the primary boot image. Please ensure that disk has
the recommended capacity for the appliance version.

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

Status: Running

3. 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.

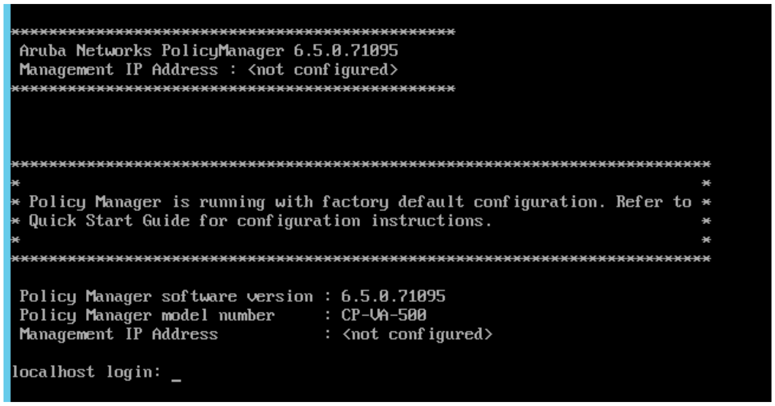
   When the rebooting process is complete, the W-ClearPass virtual appliance is configured, and the virtual appliance will power on and boot up within a couple of minutes.

NOTE

The whole process, from deploying the OVF image to the presentation of the login banner screen, typically takes between 30 and 40 minutes.

4. After the W-ClearPass virtual appliance launches correctly, the following banner is displayed:

Figure 47: *Virtual Appliance Login Banner*



```
***********************************************
 Aruba Networks PolicyManager 6.5.0.71095
 Management IP Address : <not configured>
***********************************************



**************************************************************************
*                                                                        *
* Policy Manager is running with factory default configuration. Refer to *
* Quick Start Guide for configuration instructions.                      *
*                                                                        *
**************************************************************************

 Policy Manager software version : 6.5.0.71095
 Policy Manager model number     : CP-VA-500
 Management IP Address           : <not configured>

localhost login: _
```

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 W-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**.

NOTE

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 49.

   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, which is described in the next section.

Applying and Activating the W-ClearPass License

NOTE

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.

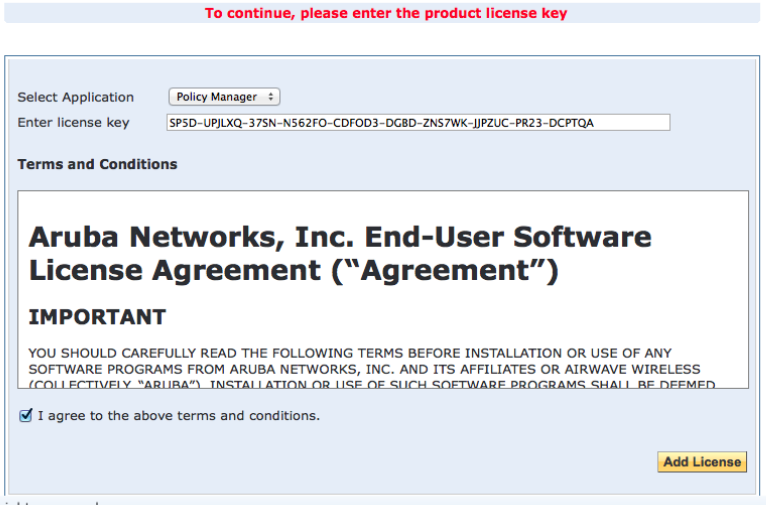
To activate and apply the W-ClearPass license:

1. After the configuration has been applied at the virtual appliance console, open a web browser and go to the W-ClearPass management interface:

   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.
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 48: *Entering the License Key*



To continue, please enter the product license key

Select Application: Policy Manager

Enter license key: SP5D-UPJLXQ-37SN-N562FO-CDFOD3-DGBD-ZNS7WK-JJPZUC-PR23-DCPTQA

Terms and Conditions

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

IMPORTANT

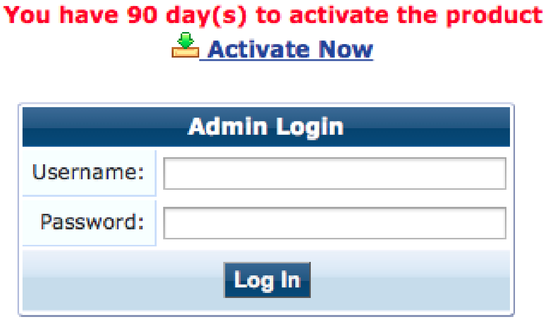
YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS BEFORE INSTALLATION OR USE OF ANY SOFTWARE PROGRAMS FROM ARUBA NETWORKS, INC. AND ITS AFFILIATES OR AIRWAVE WIRELESS (COLLECTIVELY "ARUBA"). INSTALLATION OR USE OF SUCH SOFTWARE PROGRAMS SHALL BE DEEMED

☑ I agree to the above terms and conditions.

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 49: *Activating W-ClearPass*



You have 90 day(s) to activate the product

Activate Now

Admin Login

Username:

Password:

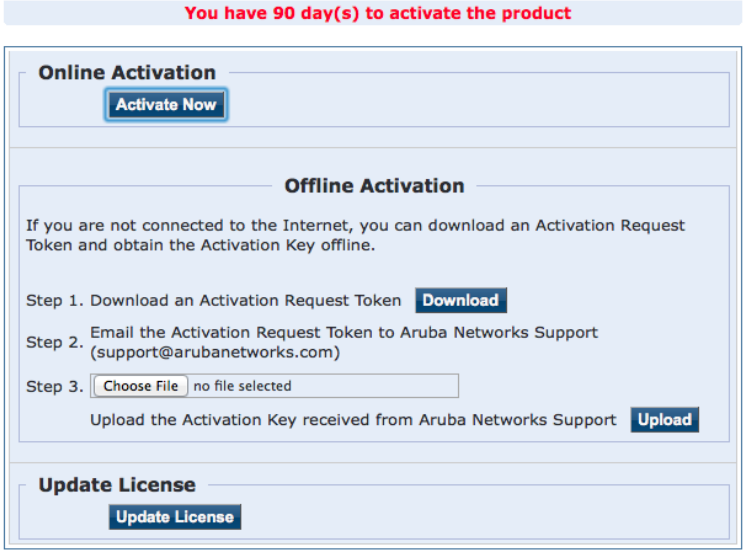
Log In

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

   When you click **Activate Now**, W-ClearPass Policy Manager attempts to activate the license over the Internet with Dell 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 50.

Figure 50: *Performing Offline Activation*



You have 90 day(s) to activate the product

Online Activation

Activate Now

Offline Activation

If you are not connected to the Internet, you can download an Activation Request Token and obtain the Activation Key offline.

Step 1. Download an Activation Request Token Download

Step 2. Email the Activation Request Token to Aruba Networks Support (support@arubanetworks.com)

Step 3. Choose File no file selected

Upload the Activation Key received from Aruba Networks Support Upload

Update License

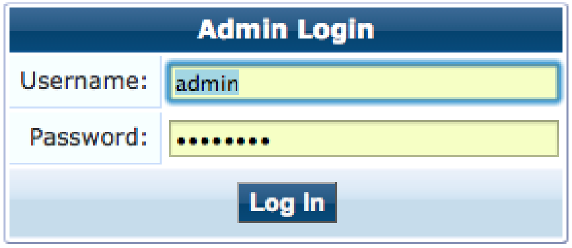
Update License

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 51: *Logging in to the W-ClearPass Virtual Appliance*



Admin Login

Username: admin

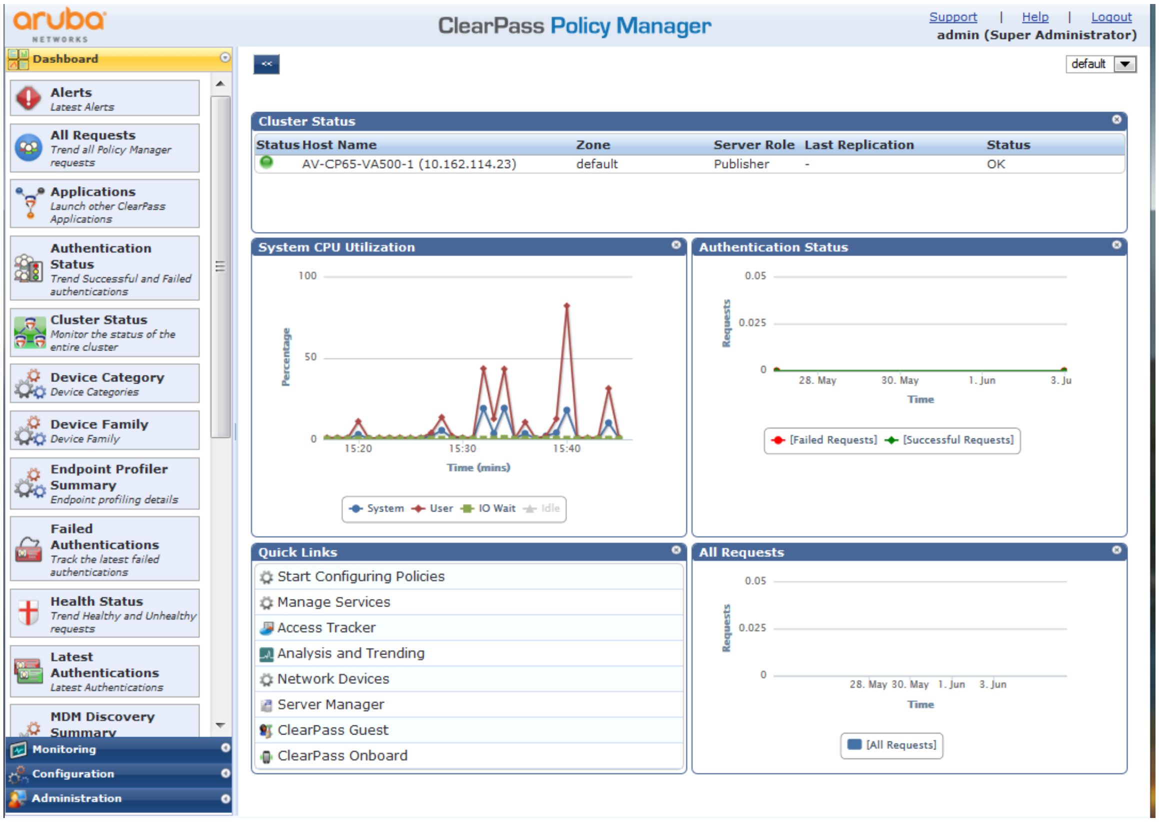
Password: ••••••••

Log In

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 45.
2. Click **Log In**.

   The W-ClearPass Policy Manager Home Page is displayed.

Figure 52: *W-ClearPass Policy Manager Home Page*



Status	Host Name	Zone	Server Role	Last Replication	Status
●	AV-CP65-VA500-1 (10.162.114.23)	default	Publisher	-	OK

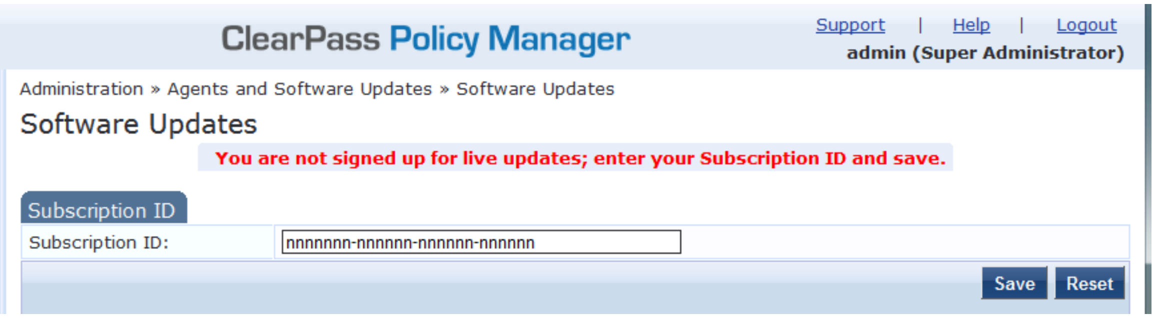
Signing Up for Live Software Updates

Upon your initial login to W-ClearPass Policy Manager, we recommend that you 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 53: *Entering the Subscription ID for Live Updates*



Administration » Agents and Software Updates » Software Updates

Software Updates

You are not signed up for live updates; enter your Subscription ID and save.

Subscription ID

Subscription ID:	nnnnnnn-nnnnnn-nnnnnn-nnnnnn

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

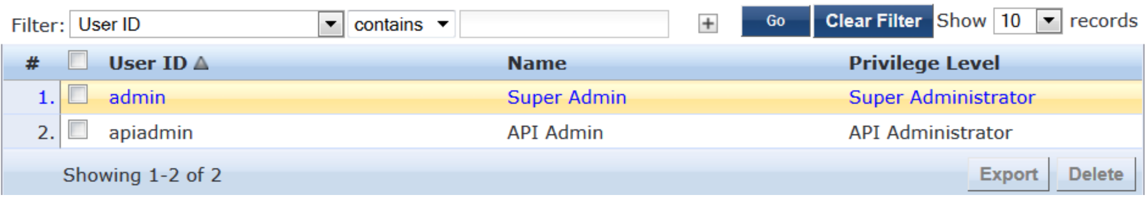
When the cluster password for this W-ClearPass server is set upon initial configuration (see Completing the Virtual Appliance Configuration on page 45), the administration password is also set to the same password. If you wish to assign a unique **admin** password, use this procedure to change it.

To change the administration password:

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

   The **Admin Users** page opens.

Figure 54: *Admin Users Page*



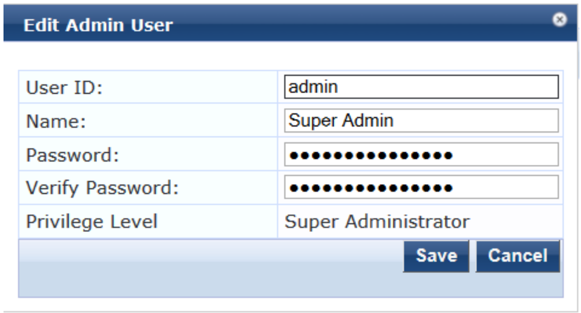
#	□	User ID △	Name	Privilege Level
1.	□	admin	Super Admin	Super Administrator
2.	□	apiadmin	API Admin	API Administrator

Showing 1-2 of 2

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

   The **Edit Admin User** dialog opens.

Figure 55: *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. 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.

Chapter 3
Maintaining W-ClearPass Services

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 W-ClearPass Policy Manager services, including any Active Directory domains to which the current server is now joined.

To access the **Services Control** page:

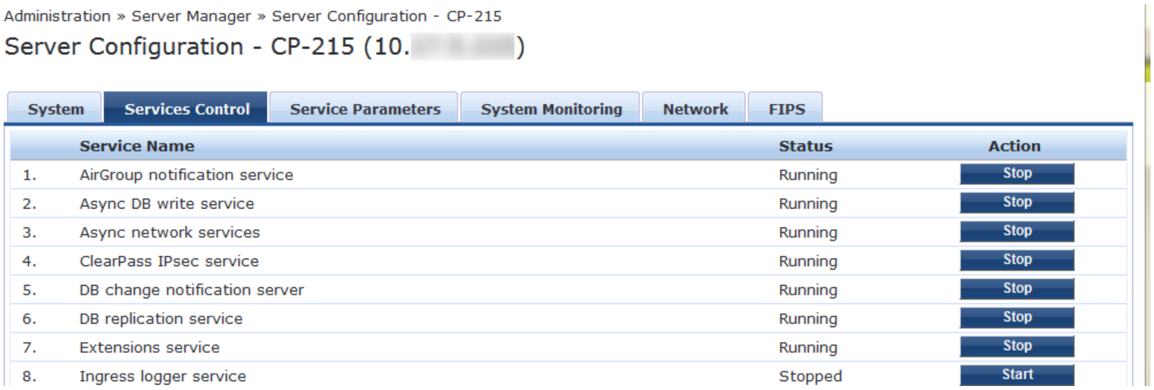
1. In W-ClearPass, navigate to **Administration > Server Manager > Server Configuration**.

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

   The **Services Control** page opens.

Figure 56: *Server Configuration > Services Control Page*



Administration » Server Manager » Server Configuration - CP-215

Server Configuration - CP-215 (10.[redacted])

	Service Name	Status	Action
1.	AirGroup notification service	Running	Stop
2.	Async DB write service	Running	Stop
3.	Async network services	Running	Stop
4.	ClearPass IPsec service	Running	Stop
5.	DB change notification server	Running	Stop
6.	DB replication service	Running	Stop
7.	Extensions service	Running	Stop
8.	Ingress logger service	Stopped	Start

NOTE

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 W-ClearPass 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 W-Policy Manager appliance.	This ensures that external Management Information Base (MIB) browsers can browse the system-level MIB objects exposed by the W-ClearPass Policy Manager appliance. The options on this page vary based on the SNMP version that you select.
Network	Use the Network page to: ● Create generic routing encapsulation (GRE) tunnels and VLANs related to guest users. ● Control which applications can have access to the node.	● 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. ● VLAN ID 1 is often reserved for use by certain network management components **NOTE:** Avoid using VLAN ID 1 unless you know it will not conflict with a VLAN already defined in your network.
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 Command Line Interface (CLI) provides a way to manage and configure W-ClearPass 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 console to run the virtual appliance.

```
****************************************************************************************
* Policy Manager CLI v6.6(0), Copyright © 2016, Aruba Networks, Inc.                *
* Software Version : 6.6.0.62080                                 *
****************************************************************************************
```

```
***************************************************************************************
* Dell ClearPass Policy Manager                                 *
* Software Version : 6.6.0.62080                                 *
***************************************************************************************
Logged in as group Local Administrator
[appadmin@company.com]#
```

CLI Task Examples

View the W-Policy Manager Data and Management Port IP Addresses 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>	● Network interface type: *mgmt* or *data* ● 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 W-Policy Manager appliance to the Active Directory domain (for more information, see Joining an Active Directory Domain on page 1).

```
[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.