

ClearPass 6.7 Getting Started Guide

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



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

This *Getting Started Guide* provides the following information:

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

About the ClearPass Access Management System

This section contains the following information:

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

ClearPass Access Management System Overview

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

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

Role-Based and Device-Based Access

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

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

Self-Service Capabilities

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

Leveraging Contextual Data

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

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

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

Third-Party Security and IT Systems

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

Supported Browsers

The supported browsers for ClearPass are:

- Mozilla Firefox on Windows 7, Windows 8.x, Windows 10, and macOS
- Google Chrome for macOS and Windows
- Apple Safari 9.x and later on macOS
- Mobile Safari 5.x on iOS
- Microsoft Edge on Windows 10
- Microsoft Internet Explorer 10 and later on Windows 7 and Windows 8.x



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

Key Features

ClearPass's key features are as follows:

- Role-based network access enforcement for multivendor Wi-Fi, wired, and VPN networks
- Virtual and hardware appliances that can be deployed in a cluster to increase scalability and redundancy.
- Support for popular virtualizations platforms such as VMware vSphere Hypervisor (ESXi), Microsoft Hyper-V, and Amazon AWS (EC2).
- Intuitive policy configuration templates and visibility troubleshooting tools.
- Supports multiple authentication/authorization sources—AD, LDAP, and SQL dB.
- Self-service device onboarding with built-in certificate authority (CA) for BYOD.
- Guest access with extensive customization, branding and sponsor-based approvals.
- Supports NAC and EMM/MDM integration for mobile device assessments.
- Comprehensive integration with the Aruba 360 Security Exchange Program.
- SAML 2.0 Identity Provider, which allows seamless single sign-on (SSO) to cloud or on-premise applications.

- SAML 2.0 Service Provider, which allows seamless and secure access to ClearPass components using federated/unified identity.
- Advanced reporting and granular alerts.
- Active and passive device fingerprinting
- High performance, scalability, High Availability, and load balancing
- A Web-based user interface that simplifies policy configuration and troubleshooting
- Network Access Control (NAC), Network Access Protection (NAP) posture and health checks, and Mobile Device Management (MDM) integration for mobile device posture checks
- Social and Cloud Identity Network and Cloud Application single sign-on (SSO) via OAuth 2.0
- Facebook, Twitter, LinkedIn, Azure Active Directory and Office 365, Google G Suite, and so on.
- Device and User certificate enrollment via Simple Certificate Enrollment Protocol (SCEP), Enrollment over Secure Transport (EST) and REST API-based workflows
- Advanced reporting of all user authentications and failures
- Enterprise Reporting, Monitoring, and Alerting
- HTTP/RESTful APIs for integration with third-party systems, Internet security, and MDM
- Device profiling and self-service onboarding
- Guest access with extensive branding and customization and sponsor-based approvals
- IPv6 administration support

Advanced Policy Management

ClearPass advanced policy management support includes:

- **Employee access**

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

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

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

- **Built-in device profiling**

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

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

- **Access for unmanaged endpoints**

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

- **Secure configuration of personal devices**

ClearPass Onboard fully automates the provisioning of any Windows, macOS, iOS, Android, ChromeOS, and Ubuntu devices via a built-in enrollment workflow.

Valid users are redirected to a template-based interface to configure required SSIDs and 802.1X settings, and download unique device credentials.

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

- **Customizable visitor management**

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

- **Device health checks**

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

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

ClearPass Policy Manager Hardware and Virtual Appliances

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

- For hardware and virtual appliance installation and deployment procedures, see [ClearPass 6.7 Getting Started Guide](#).

Virtual appliances are supported on the following platforms:

- VMware ESX and ESXi

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

- Microsoft Hyper-V

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

ClearPass Specifications

Hardware and Virtual Appliances

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

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

ClearPass Platform

- Deployment templates for any network type, identity store, and endpoint
- 802.1X, MAC authentication and captive portal support
- ClearPass OnConnect for SNMP-based enforcement on wired switches
- Advanced reporting, analytics and troubleshooting tools
- Interactive policy simulation and monitor mode utilities
- Multiple device registration portals—Guest, Aruba AirGroup, BYOD (bring your own device), and unmanaged devices

- Admin/Operator access security via CAC (Common Access Card) and TLS (Transport Layer Security) certificates

Framework and Protocol Support

- RADIUS, RADIUS CoA, TACACS+, Web authentication, and SAML v2.0
- EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
- PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public)
- EAP-TTLS (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-MD5, PAP, CHAP)
- EAP-TLS
- PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5
- Wireless and wired 802.1X and VPN
- OAuth .02
- Microsoft NAP and NAC
- Active Directory machine authentication
- Online Certificate Status Protocol (OCSP)
- SNMP generic MIB, SNMP private MIB
- Common Event Format (CEF), Log Event Extended Format (LEEF)
- Simple Certificate Enrollment Protocol (SCEP)
- Enrollment over Secure Transport (EST)

Supported Identity Stores

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

IPv6 Support

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

Profiling Methods

- Active: Nmap, WMI, SSH, SNMP

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

Setting Up the ClearPass Hardware Appliances

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

This section contains the following information:

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

About the ClearPass Hardware Appliances

Aruba provides three hardware appliance platforms:

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

Table 1: Functional Description of the ClearPass Hardware Appliance Ports

Port	Description
Data port (Gigabit Ethernet)	The Data port (ethernet 1) provides a point of contact for RADIUS, TACACS+, Web authentication, and other dataplane requests. This configuration is optional. If this port is not configured, requests are redirected to the Management port.
iLO port	The iLO (Integrated Lights-Out) port is an Ethernet port that provides out-of-band management facilities. The iLO port makes it possible to perform activities on the ArubaOS switch or an HP server from a remote location. The iLO card has a separate network connection (and its own IP address) to which one can connect via HTTPS. Available on the ClearPass C2000 and C3000 hardware appliances.
Management port (Gigabit Ethernet)	The Management port (ethernet 0) provides access for cluster administration and appliance maintenance using the WebUI, CLI, or internal cluster communication. This configuration is mandatory.

Port	Description
Serial port	The Serial port is used to initially configure the ClearPass hardware appliance using a hard-wired terminal.
SPAN ports	A SPAN (Switched Port Analyzer) port is a method of monitoring network traffic. The switch sends a copy of all network packets seen on one port (which is the <i>monitored</i> or <i>source</i> port) to a destination SPAN port, where the packets can be analyzed. Available on the ClearPass C3000 hardware appliance.
USB ports	Two USB v2.0 ports are provided on each ClearPass hardware appliance.
VGA connector	You can use the VGA Connector to connect the ClearPass hardware appliance to a monitor and keyboard.

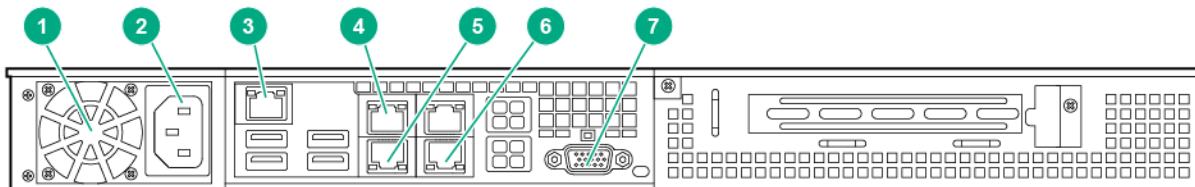
ClearPass C1000 Hardware Appliance

The ClearPass Policy Manager C1000 hardware appliance (SKU: JZ508A) is a RADIUS/ TACACS+ server that provides advanced policy control for up to 500 simultaneous sessions.

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

[Figure 1](#) shows the ports and components on the rear panel of the ClearPass C1000 hardware appliance. The function of each of these ports and components is described in [Table 1](#).

Figure 1 Ports and Components on the ClearPass C1000 Hardware Appliance



Callout Number	C1000 Port/Component
1	Fan
2	Power Supply
3	Serial port
4	Data port

Callout Number	C1000 Port/Component
5	Management port (eth0)
6	USB ports (2)
7	VGA Connector

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

[Table 2](#) provides the specifications for the ClearPass Policy Manager C1000 hardware appliance.

Table 2: *ClearPass C1000 Appliance Specifications*

ClearPass C1000 Appliance	Specifications
Hardware Model	Unicom S-1200 R4
CPU	(1) Eight Core 2.4 GHz Atom C2758
Memory	8 GB (2 x2 GB)
Hard drive storage	<ul style="list-style-type: none"> (1) SATA (7.3K RPM), Serial ATA 1 TB hard drive
Serial Port	Yes: RJ-45
Performance & Scale	Please refer to the <i>ClearPass Scaling & Ordering Guide</i>
Form Factor	
Rack mount	Included
Dimensions (WxHxD)	17.2" x 1.7" x 11.3"
Weight (max configuration)	8.5 lbs
Power	
Power consumption (maximum)	200 watts
Power supply	Single
AC input voltage	100/240 VAC auto-selecting

ClearPass C1000 Appliance	Specifications
AC input frequency	50/60 Hz auto-selecting
Environmental	
Operating temperature	5° C to 35° C (41° F to 95° F)
Operating vibration	0.26 G at 5 Hz to 200 Hz for 15 minutes
Operating shock	1 shock pulse of 20 G for up to 2.5 ms
Operating altitude	-16 m to 3,048 m (-50 ft to 10,000 ft)

ClearPass C2000 Hardware Appliance

The ClearPass Policy Manager C2000 hardware appliance (SKU: JZ509A) is a RADIUS/ TACACS+ server that provides advanced policy control for up to 5,000 simultaneous sessions.

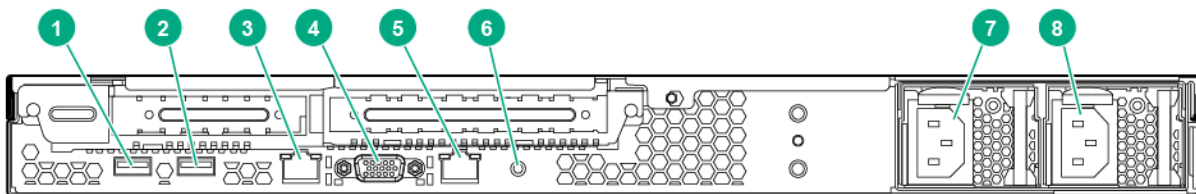
The ClearPass C2000 appliance ships with two x 1TB SATA disk drives. These drives are managed by an LSI RAID-1 controller. The drives are configured as a RAID-1 pair. The LSI controller presents to ClearPass a single virtual 1TB drive, masking the two underlying physical drives.

[Figure 2](#) shows the ports and components on the rear panel of the ClearPass C2000 hardware appliance. The function of each of these ports and components is described in [Table 1](#).



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

Figure 2 Ports and Components on the ClearPass C2000 Hardware Appliance



Callout Number	C2000 Port/Component
1 and 2	USB ports (2)
3	iLO (Integrated Lights-Out) port and Management port (eth0)
4	VGA Connector
5	Data port (eth1)

Callout Number	C2000 Port/Component
6	<p>UID (Unit ID)</p> <p>The UID LED helps you identify and locate a system, especially in high-density rack environments. Additionally, the UID is used to indicate that a critical operation is underway on the host, such as Remote console access or ROM flash.</p> <p>The "current state" (on or off) of the UID is the last state chosen using one of these methods. If a new state is chosen while the UID is blinking, this new state becomes the current state, and takes effect when the UID stops blinking.</p> <p>NOTE: The Unit ID Light web page does not automatically refresh itself if the state of the actual light changes after the page is loaded. To ensure the page accurately reflects the state of the UID Light, click on the Virtual Indicators link to update the page.</p>
7	Power Supply
8	Optional redundant Power Supply

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

[Table 3](#) provides the specifications for the ClearPass C2000 hardware appliance.

Table 3: *ClearPass C2000 Appliance Specifications*

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

ClearPass C2000 Appliance	Specifications
Dimensions (WxHxD)	17.11" x 1.70" x 150.5"
Weight (max configuration)	Up to 19.18 lbs
Power Specifications	
Power consumption (maximum)	250 watts
Power supply	HPE 900W AC 240 VDC Power Input FIO Module NOTE: The optional HPE 900W Redundant Power Supply supports 100 VAC to 240 VAC; this power supply also supports 240 VDC.
Power redundancy	Optional
AC input voltage	100/240 VAC auto-selecting
AC input frequency	50/60 Hz auto-selecting
Environmental Specifications	
Operating temperature	10° C to 35° C (50° F to 95° F)
Operating vibration	Random vibration at 0.000075 G ² /Hz, 10Hz to 300Hz, (0.15 G's nominal)
Operating shock	2 G's
Operating altitude	3,050 m (10,000 ft)

ClearPass C3000 Hardware Appliance

The ClearPass Policy Manager C3000 hardware appliance (SKU: JZ510A) is a RADIUS/ TACACS+ server that provides advanced policy control for up to 25,000 simultaneous sessions.

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

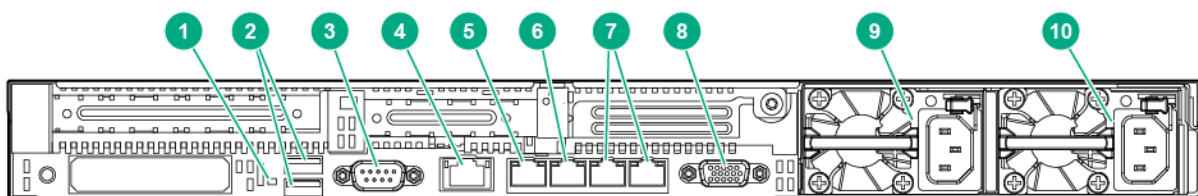
The LSI controller presents to ClearPass a single virtual 1.675 TB drive, masking the underlying two physical drive groups (two groups of two mirrored drives).

[Figure 3](#) shows the ports and components on the rear panel of the ClearPass C3000 hardware appliance. The function of each of these ports and components is described in [Table 1](#).



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

Figure 3 Ports and Components on the ClearPass C3000 Hardware Appliance



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

[Table 4](#) provides the specifications for the ClearPass C3000 hardware appliance.

Table 4: *ClearPass C3000 Appliance Specifications*

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

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

Before Starting the ClearPass Installation

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

Table 5: *ClearPass Server Configuration Reference*

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

Configuring the ClearPass Hardware Appliance

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

To configure the ClearPass Policy Manager hardware appliance:

1. Connect the Serial port.

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

The hardware appliance is now available for configuration.

2. Configure the Serial port.

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

3. Log in.

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

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

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

This initiates the Policy Manager configuration wizard.

4. Configure the ClearPass hardware appliance.

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

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

5. Specify the cluster password.



Setting the cluster password also changes the password for the CLI user **appadmin**, as well as the Administrative user **admin**. If you want the **admin** password to be unique, see [Changing the Administration Password on page 18](#).

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

6. Configure the system date and time.

- Follow the prompts to configure the system date and time.
- To set the date and time by configuring the NTP server, use the primary and secondary NTP server information you entered in [Table 5](#).

7. Apply the configuration.

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

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

Activating ClearPass

To activate ClearPass Policy Manager and apply the ClearPass license:

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

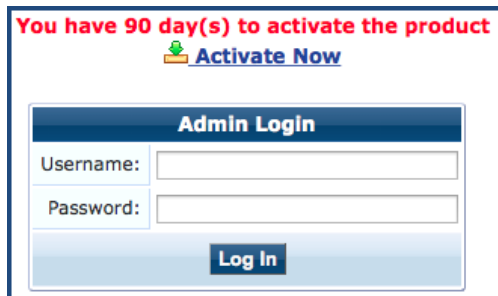
<https://x.x.x.x/tips/>

where **x.x.x.x** is the IP address of the management interface defined for the ClearPass server as listed in [Table 5](#).

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

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

Figure 4 *Activating ClearPass*



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

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

If the ClearPass Policy Manager hardware appliance does not have Internet access, you can perform the product activation offline by following the steps for offline activation presented in the **Offline Activation** section shown in [Figure 5](#).

Figure 5 *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. no file selected

Upload the Activation Key received from Aruba Networks Support **Upload**

Update License

Update License

4. If the ClearPass server is connected to the Internet, click the **Activate Now** button.
You receive the message, "Product has been successfully activated" and the **Admin Login** dialog is displayed.

Logging in to the ClearPass Hardware Appliance

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

Figure 6 *Logging in to the ClearPass Hardware Appliance*

Admin Login

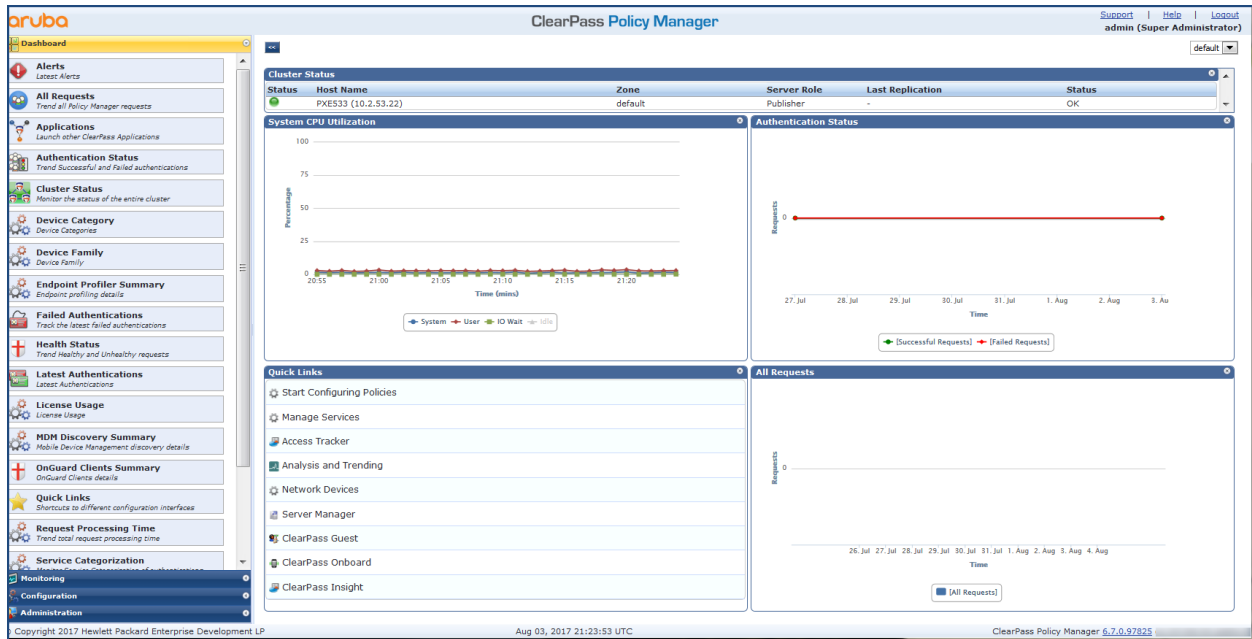
Username:

Password:

Log In

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

Figure 7 ClearPass Policy Manager Landing Page



Changing the Administration Password

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

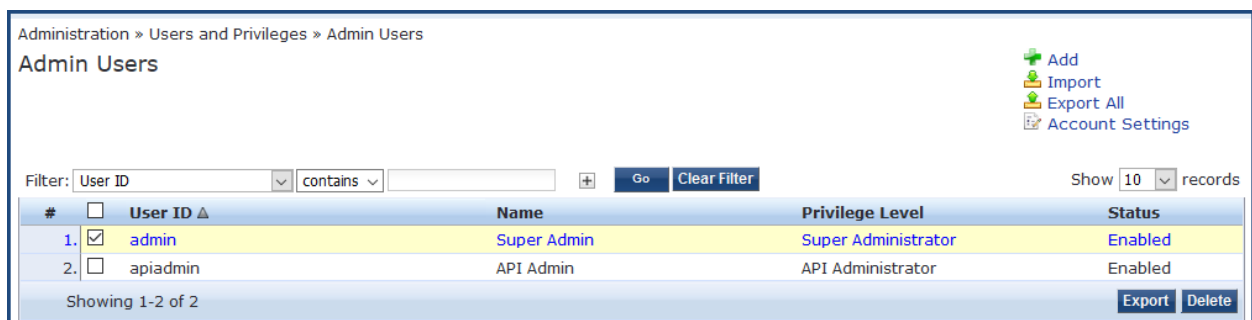
If you wish to assign a unique **admin** password, use this procedure to change it.

To change the administration password:

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

The **Admin Users** page opens.

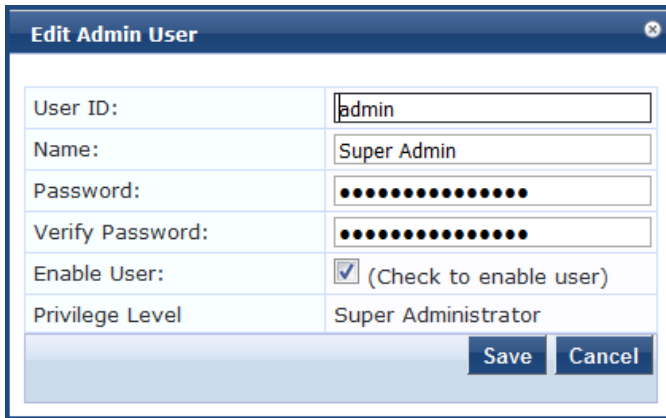
Figure 8 Admin Users Page



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

The **Edit Admin User** dialog opens.

Figure 9 *Changing the Administration Password*



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

Powering Off the ClearPass Hardware Appliance

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

To power off the ClearPass hardware appliance:

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

The ClearPass hardware appliance shuts down.



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

Resetting the System Passwords to the Factory Defaults

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

Generating the Password Recovery Key

To generate the password recovery key:

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

The system prompts you with the following choices:

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

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

Resetting the System Account Passwords to the Factory Defaults

To reset the administrator password:

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

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

3. To reset the system account passwords to the factory default values, enter **y**.
4. You can now log in with the new administrator password emailed to you by Aruba Technical Support.

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

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

This section contains the following information:

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

Introduction

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

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

Meeting the Recommended vSphere Hypervisor Server Specifications

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

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

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

Supplemental Storage/Hard Disk Requirement

All VMware vSphere Hypervisor virtual machines use hardware version 8.

ClearPass VMware ships with a 30 GB hard disk volume. This must be supplemented with additional storage/hard disk by adding a virtual hard disk (see [Adding a Virtual Hard Disk on page 26](#) for details). The additional space required depends on the ClearPass virtual appliance version.

Processing and Memory Requirements

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

ClearPass Server I/O Rate

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



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

Supported Hypervisors

ClearPass supports the following hypervisors:

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

Virtual Appliance Platforms

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

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

Before Starting the ClearPass Installation

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

Table 6: *ClearPass Server Configuration Information*

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

vSphere Web Client ClearPass Installation Overview

ClearPass VMware software packages are distributed as Zip files.

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

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



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

3. Add a new hard disk, based on the requirements for your type of virtual machine.
4. Power on and configure the virtual appliance.

ClearPass VMware Virtual Appliance Installation Setup

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

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



Release Notes are available in the appropriate version folder under **Aruba Support Center > Documentation > Software User & Reference Guides > ClearPass > Release Notes**.

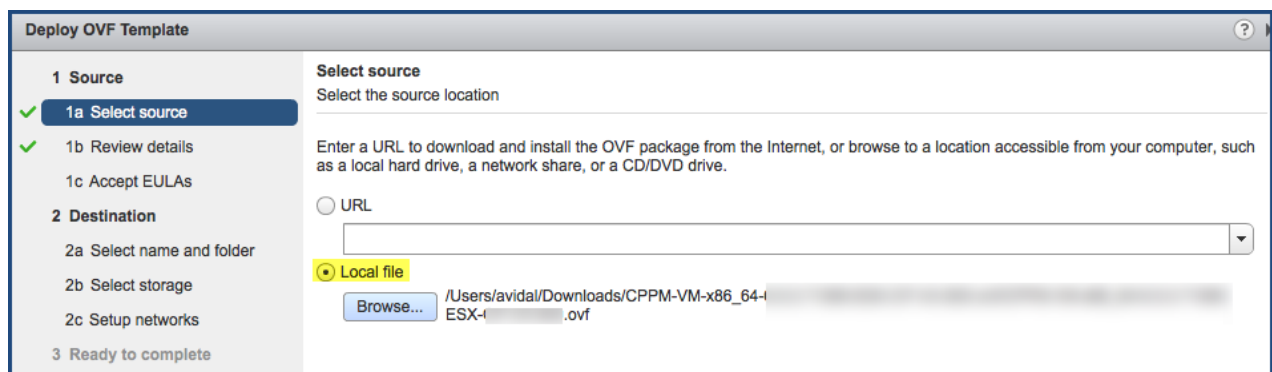
2. Then check the recommended virtual hardware specifications and verify that your system meets those requirements.
3. Start the VMware vSphere Web Client.
4. Extract the files into a folder on your desktop.
5. Using either the VMware vSphere Web Client or the standard vSphere Client, deploy the Open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

The Deploy OVF Template opens.



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

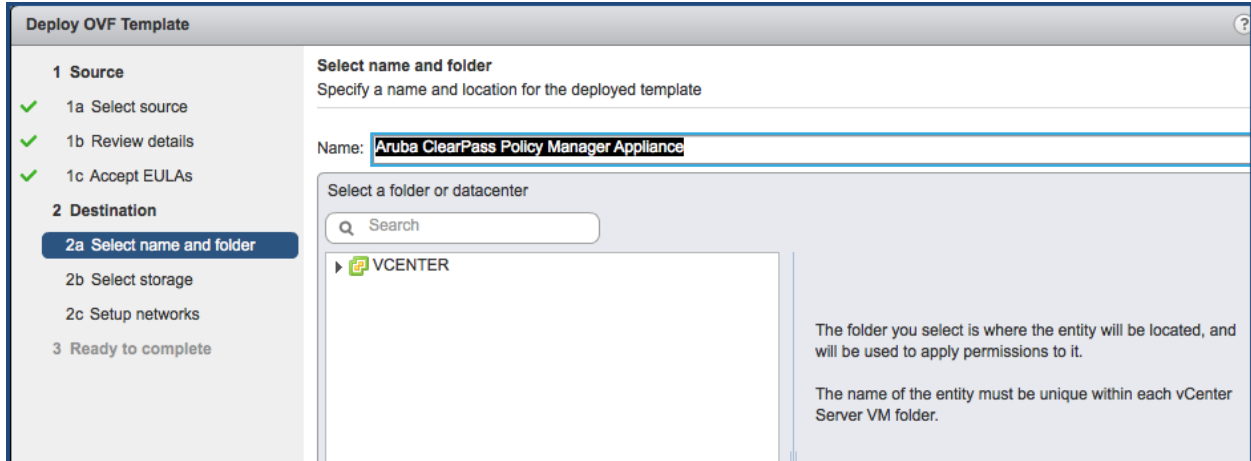
Figure 10 Deploy OVF Template: Selecting the Source Location



6. Select **Local File**, then click **Browse**.
7. Navigate to the folder where you extracted the files, then click **Next**.

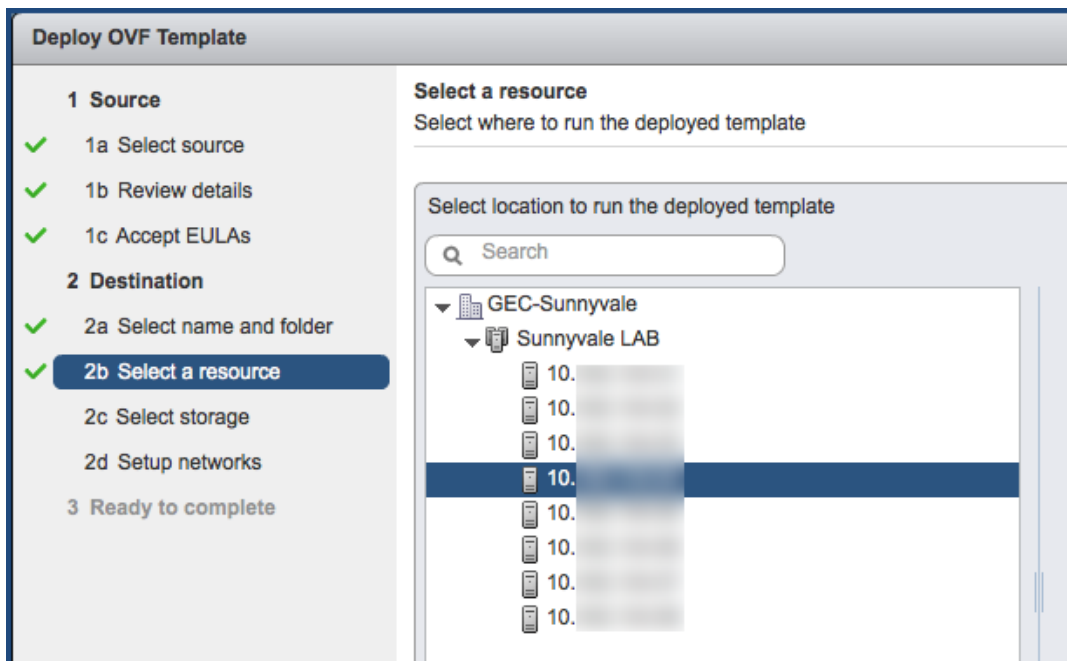
- The **Review Details** screen opens.
8. Review the information presented, then click **Next**.
The **Accept EULAs** screen opens.
 9. Read the End User License Agreements (EULA) and click **Accept**, then click **Next**.
The **Select Name and Folder** screen opens.

Figure 11 *Selecting the Name and Location for the Deployed Template*



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

Figure 12 *Selecting a Resource*



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

Figure 13 *Selecting the Location to Store the Files*

The screenshot shows the 'Deploy OVF Template' wizard at the 'Select storage' step. The left sidebar shows the progress: 1 Source (1a Select source, 1b Review details, 1c Accept EULAs), 2 Destination (2a Select name and folder, 2b Select storage), and 3 Ready to complete. The '2b Select storage' step is active. The main area is titled 'Select storage' with the instruction 'Select location to store the files for the deployed template'. It includes a 'Select virtual disk format:' dropdown set to 'Thin Provision' and a 'VM Storage Policy:' dropdown set to 'None'. Below this is a table of accessible datastores:

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

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



The virtual disk format specified in Figure 13 is **Thin Provision**. In a production environment, to ensure that the virtual appliance will not run out of disk space, Aruba recommends using the **Thick Lazy Zeroed** virtual disk format.

The **Setup Networks** screen appears.

Figure 14 *Configuring the Networks for VM Deployment*

The screenshot shows the 'Deploy OVF Template' wizard at the 'Setup networks' step. The left sidebar shows the progress: 1 Source (1a Select source, 1b Review details, 1c Accept EULAs), 2 Destination (2a Select name and folder, 2b Select storage, 2c Setup networks), and 3 Ready to complete. The '2c Setup networks' step is active. The main area is titled 'Setup networks' with the instruction 'Configure the networks the deployed template should use'. It features a table with 'Source' and 'Destination' columns. The first row shows 'VM Network' mapped to 'VLAN110'. Below the table, 'IP protocol:' is set to 'IPv4' and 'IP allocation:' is set to 'Static - Manual'. At the bottom, there are sections for 'Source: VM Network - Description' (The VM Network network) and 'Destination: VLAN110 - Protocol settings'.

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

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

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

The OVF file is deployed in the selected network.

Adding a Virtual Hard Disk

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

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

Figure 15 *Virtual Appliance Summary Tab*

Aruba ClearPass Policy Manager Appliance

Getting Started **Summary** Monitor Manage Related Objects

Powered Off

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.

Launch Console

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	—

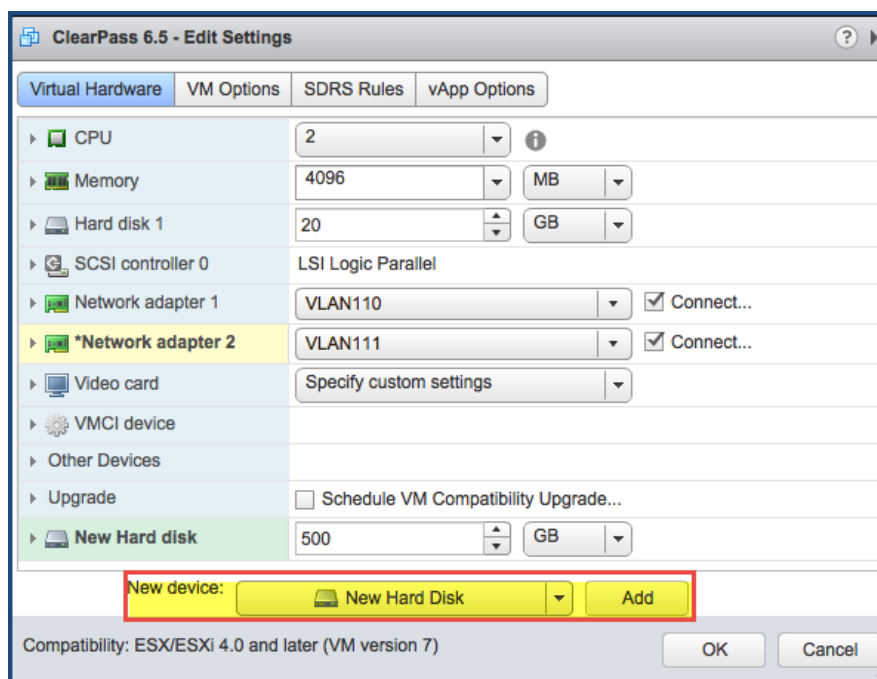
Tags

Assigned Tag	Category
This list is empty.	

Edit Settings.

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

Figure 16 *Editing the Virtual Machine Settings*

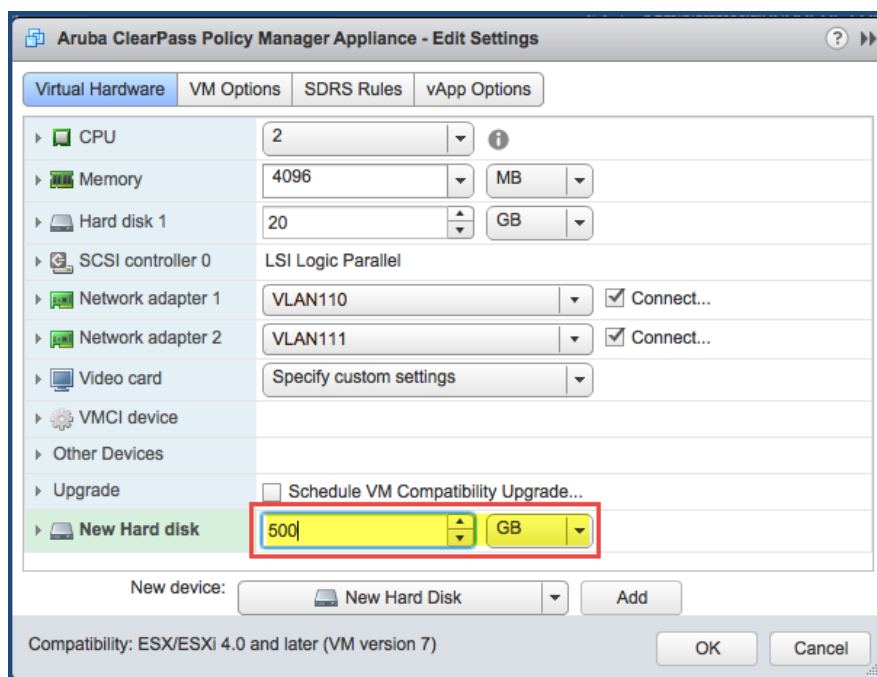


3. Add a new virtual hard disk:

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

The **Virtual Hardware** dialog opens.

Figure 17 *Specifying the Size of the New Hard Disk*



- Specify the size of the new hard disk (as shown in [Figure 17](#)), then click **OK**.



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

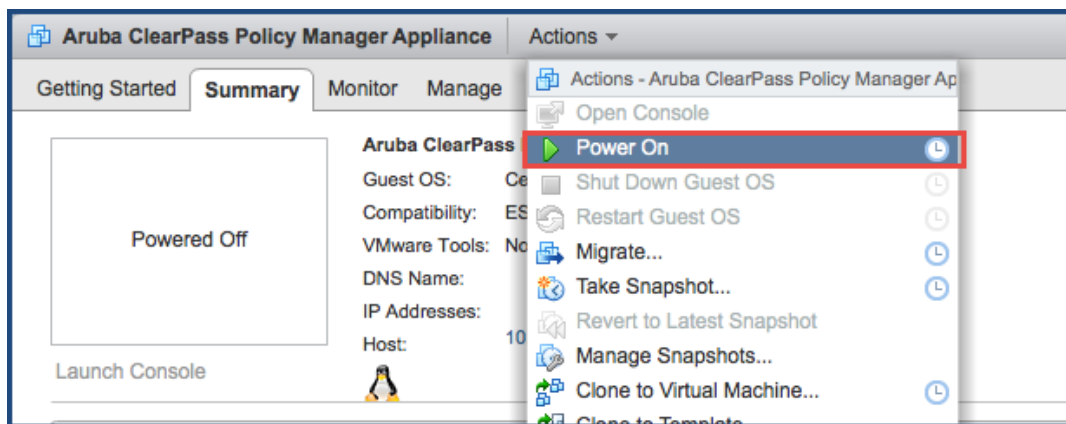
4. Make sure that the network adapters are assigned correctly:
 - a. **Network adapter 1: Management port**
 - b. **Network adapter 2: Data port**
 - c. Click **OK**.

Launching the ClearPass Virtual Appliance

To launch the ClearPass virtual appliance:

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

Figure 18 *Powering on the Virtual Machine*



The virtual appliance is now powered on.

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

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

Enter 'y' or 'Y' to proceed:
3. To proceed, enter **y**.

ClearPass setup and installation begins.
The console screen appears.
4. Enter the **number** for the appropriate appliance type (do not enter the appliance model itself).

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

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

The system requirements are displayed for the appliance model you entered, along with your current system configuration.
5. Compare these to make sure your system meets the new system requirements.
6. When you have verified that your system meets the new requirements, press **y**.

ClearPass will reboot at least once.

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

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

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

Completing the Virtual Appliance Setup

To complete the virtual appliance setup:

1. Refer to and note the required ClearPass server configuration information listed in [Table 6](#).
2. **Log in to the virtual appliance** using the following preconfigured credentials:
 - login: **appadmin**
 - password: **<password>**

This initiates the Policy Manager Configuration wizard.

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

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

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

4. **Specify the cluster password.**



Setting the cluster password also changes the password for the CLI user **appadmin**, as well as the Administrative user **admin**. If you want the **admin** password to be unique, see [Changing the Administration Password on page 36](#).

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

Initial Login and Activation of the ClearPass Platform License

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

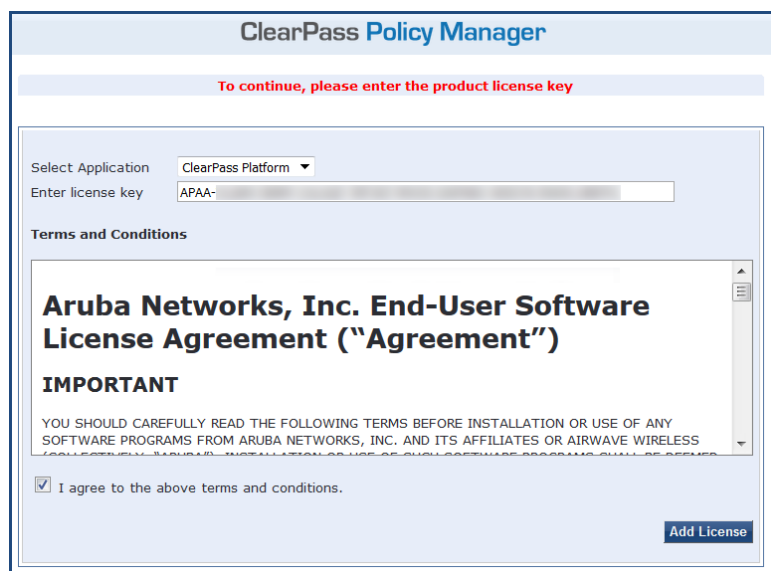
The ClearPass Platform License is the base-level license. Each ClearPass server has one ClearPass Platform License for the physical hardware. Virtual devices have a ClearPass Platform License as well on a per-expected device level.

To specify the ClearPass Platform license upon initial login:

1. After the configuration has been applied at the virtual appliance console, open a web browser and go to the management interface of ClearPassPolicy Manager: **https://x.x.x.x/tips/**, where **x.x.x.x** is the IP address of the management interface defined for the ClearPass server in [Table 6](#).
2. Log in to the ClearPass 6.7 server.
3. Accept any security warnings from your browser regarding the self-signed SSL certificate, which comes installed in ClearPass by default.

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

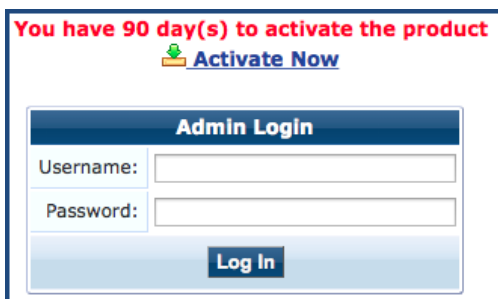
Figure 19 *Entering the ClearPass Platform License Key*

The screenshot shows the 'ClearPass Policy Manager' web interface. At the top, a red banner reads 'To continue, please enter the product license key'. Below this, there is a 'Select Application' dropdown menu set to 'ClearPass Platform'. Underneath, the 'Enter license key' field contains 'APAA-' followed by a masked area. A 'Terms and Conditions' section is expanded, showing the 'Aruba Networks, Inc. End-User Software License Agreement ("Agreement")'. It includes an 'IMPORTANT' notice and a checkbox labeled 'I agree to the above terms and conditions.' which is checked. An 'Add License' button is visible at the bottom right of the form.

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

Upon successfully entering the Platform License Key, the **Admin Login** screen appears with a message indicating that you have 90 days to activate the product and a link to activate the product.

Figure 20 *Activating ClearPass*

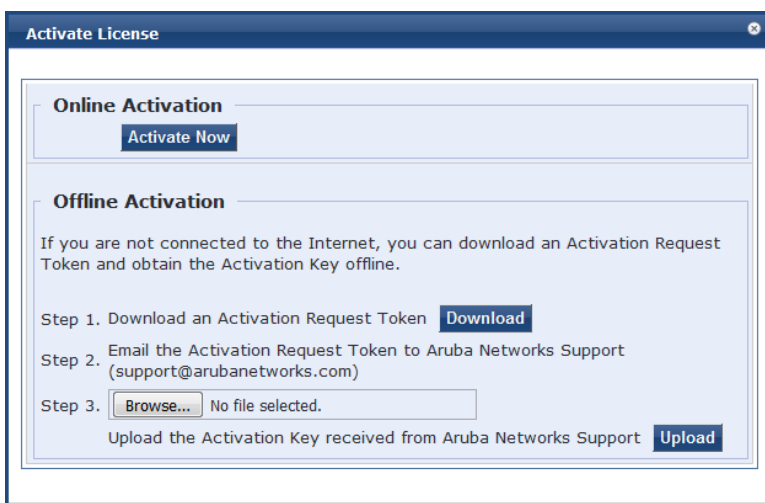


7. To activate ClearPass on this virtual appliance, click **Activate Now**.

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

If the ClearPassPolicy Manager virtual appliance does not have Internet access, you can perform the license activation offline by following the steps for offline activation presented in the **Offline Activation** section shown in [Figure 21](#).

Figure 21 *Performing Offline Activation*

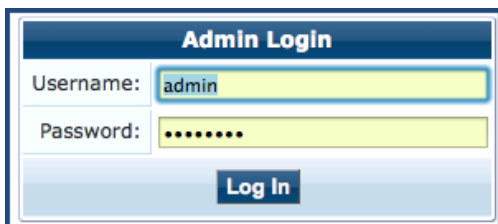


After successfully activating ClearPass online, you will see a message above the **Admin Login** screen indicating that the product has been successfully activated.

Logging in to the ClearPass Virtual Appliance

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

Figure 22 *Logging in to the ClearPass Virtual Appliance*

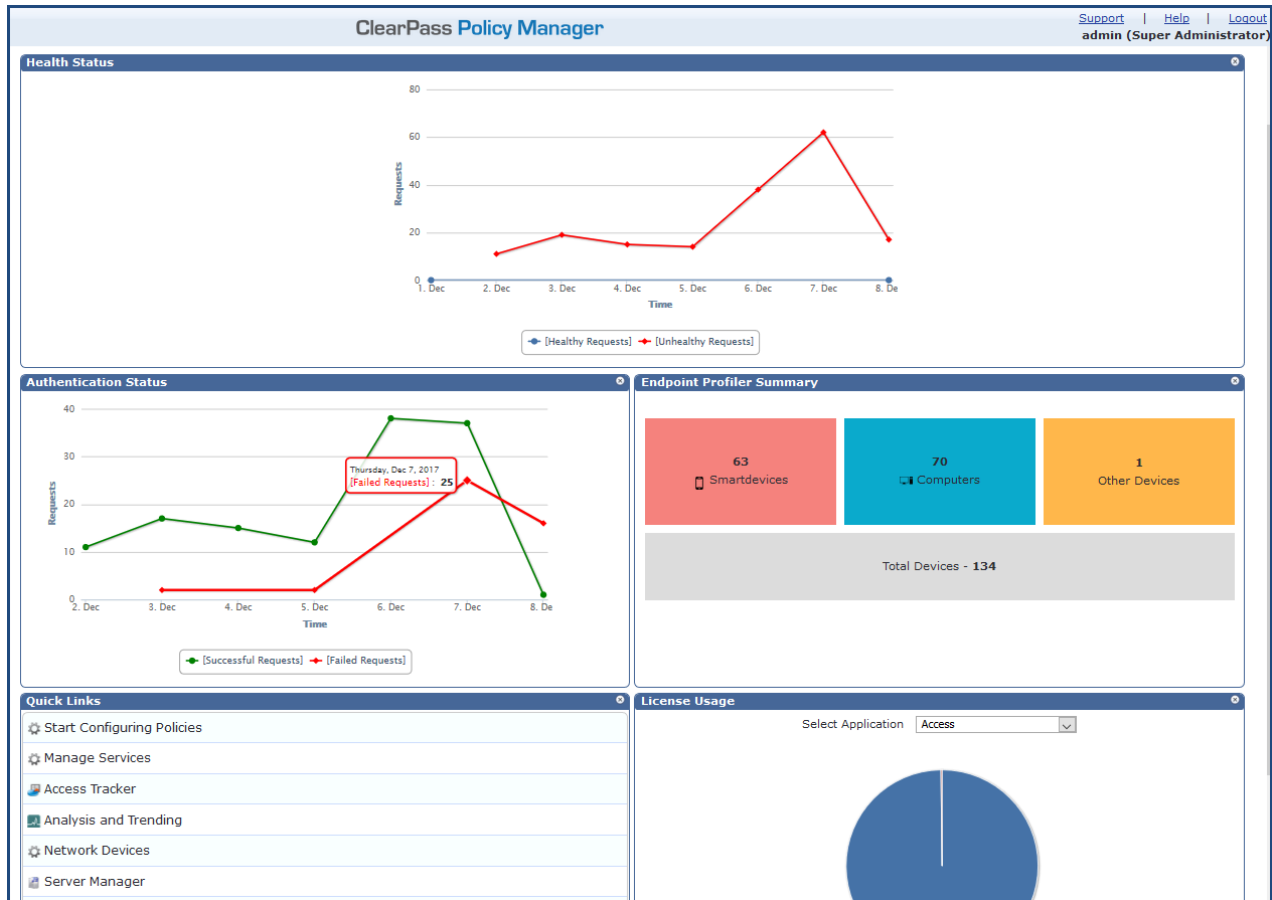


1. Log in to the ClearPass virtual appliance with the following credentials:
 - **Username:** admin
 - **Password:** Enter the cluster password defined in [Completing the Virtual Appliance Setup on page 29](#).

2. Click **Log In**.

The ClearPass Policy Manager opens.

Figure 23 ClearPass Policy Manager Landing Page



About Software Updates

This section describes the ClearPass server software update process.

ClearPass checks for available updates to the ClearPass Webservice server. The administrator can download and install these updates directly from the **Software Updates** page (depending on the Cluster-Wide Parameter settings for those parameters). Use the **Software Updates** page to register for and receive live updates for:

- **Posture Signature updates**
These updates include AntiVirus version updates. The ClearPass server uses these updates to check if the versions of the AntiVirus and the DAT file are the latest version.
- **Windows Hotfixes updates**
These updates include a list of available Windows Hotfixes for supported Windows operating systems. The ClearPass server uses these updates to show a list of the available hotfixes in the Windows Hotfixes health class.
- **Endpoint Profile Fingerprints updates**
These updates include fingerprints and are used by ClearPass in profiling endpoints.



Automatic download and installation for these three types of updates are not enabled by default (see [General Parameters](#) for more information).

You can also:

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

Software Updates Page

To update the software on the current ClearPass server:

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

[Figure 24](#) displays the **Software Updates** page:

Figure 24 *Software Updates Page*

Administration » Agents and Software Updates » Software Updates

Software Updates

Cluster Upgrade
Cluster Update
Check Status Now

HPE Passport Credentials

Username:

Password:

Save

Posture & Profile Data Updates

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

Import Updates

* Automatic download and install is disabled
To manually import Posture & Profile Data Updates, refer to Help for this page.

Firmware & Patch Updates

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

Import Updates

* Needs Restart
* Restarts Administration UI
‡ Last Installed, available for Re-Install

Check Status Now

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

Table 7: Software Updates Page Parameters

Parameter	Action/Description
HPE Passport Credentials	
HPE Passport Credentials	<p>Enter the HPE Passport Credentials provided to you.</p> <p>This text box is enabled only on a Publisher node.</p> <p>The first time the HPE Passport Credentials are saved, the ClearPass server performs the following operations:</p> <ul style="list-style-type: none"> • Contacts the Webservice server to download the latest Posture & Profile Data updates (depending on the Cluster-Wide Parameter settings for those parameters). • Checks for any available firmware and patch updates.
Posture & Profile Data Updates	
Import Updates	<p>To download the Posture and Profile Data Updates to the client (for example, a Windows laptop):</p> <ol style="list-style-type: none"> 1. From the client device, log in to the Aruba Support Center. 2. Select the Download Software tab, then navigate to ClearPass > Tools > Posture & Profile Data Updates. 3. Click the desired update(s) (which are in zip file format) and save the file. 4. From ClearPass, click the Posture and Profile Data Updates > Import Updates button to import the downloaded file into ClearPass. <p>NOTE: In a ClearPass cluster, the Import Updates option is available on the Publisher node only.</p> <p>By default, updates for Posture Signature, Windows Hotfixes, and Endpoint Profile Fingerprints are <i>not</i> automatically downloaded and installed. To set these updates to be automatic, you must set the following Cluster-Wide Parameters to TRUE:</p> <ul style="list-style-type: none"> • Automatically download Posture Signature and Windows Hotfixes Updates • Automatically download Endpoint Profile Fingerprints
Firmware & Patch Updates <p>NOTE: The Firmware & Patch Updates table shows only the data that is known to Webservice or imported using the Import Updates button.</p> <p>NOTE: Patch residual files under <code>/var/avenda/platform/backup</code>, <code>/var/avenda/platform/patches</code>, and <code>/var/avenda/platform/store/updates</code> seven days old and older are automatically deleted daily.</p>	
Import Updates	<p>If the server is not able to reach the Webservice server, click Import Updates to import the latest signed Firmware and Update patch binaries (obtained via support or other means) into this server.</p>

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

Changing the Administration Password

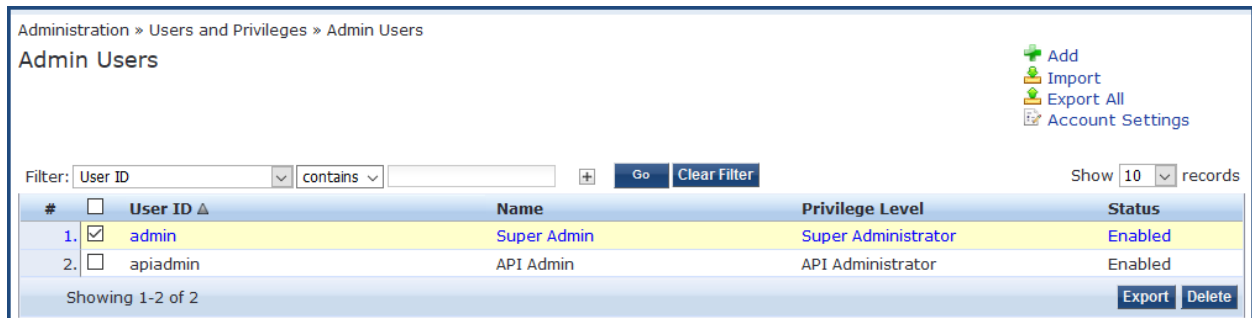
When the cluster password for this ClearPass server is set upon initial configuration (see [Completing the Virtual Appliance Setup on page 29](#)), the administration password is also set to the same password. If you wish to assign a unique **admin** password, use this procedure to change it.

To change the administration password:

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

The **Admin Users** page opens.

Figure 25 Admin Users Page

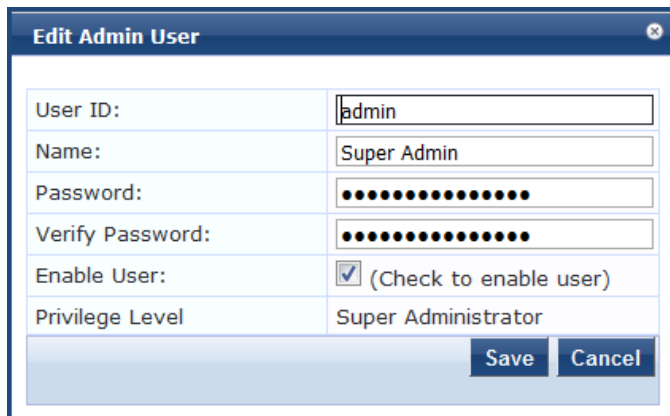


#	User ID	Name	Privilege Level	Status
1.	<input checked="" type="checkbox"/> admin	Super Admin	Super Administrator	Enabled
2.	<input type="checkbox"/> apiadmin	API Admin	API Administrator	Enabled

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

The **Edit Admin User** dialog opens.

Figure 26 Changing the Administration Password



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

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

Powering Off the ClearPass Virtual Appliance

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

To power off the ClearPass virtual appliance:

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

The ClearPass virtual appliance shuts down.

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

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

This section contains the following information:

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

Introduction

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




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

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

Supported Hypervisors

ClearPass supports the following hypervisors:

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

Meeting the Recommended Hyper-V Server Specifications

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

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

Supplemental Storage/Hard Disk Requirements

ClearPassHyper-V ships with a 30 GB hard disk volume. This must be supplemented with additional storage/hard disk by adding a virtual hard disk (see [Adding a Hard Disk to a Virtual Machine on page 43](#) for details). The additional space required depends on the ClearPass virtual appliance version.

Processing and Memory Requirements

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

ClearPass Server I/O Rate

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

Virtual Appliance Platforms

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

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

Before Starting the ClearPass Installation

Before starting the installation and configuration procedures for the virtual appliance, determine the following information for the ClearPass server on your network, note the corresponding values for the parameters listed in [Table 8](#), and keep it for your records:

Table 8: *ClearPass Server Configuration Information*

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

ClearPass Hyper-V Virtual Appliance Installation Summary

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

1. Download the Microsoft Hyper-V package from the **Download Software > ClearPass > Policy Manager > <Current_Release_Number> > Hyper-V** folder on the Aruba Support Center and unzip it to a folder on your server to extract the files.
2. Import the virtual machine.
 - a. Choose the import type.
 - b. If required, specify the virtual switch that the Management Interface and Data Interface will be connected to.
3. Add a new virtual hard disk.

- a. Configure the disk format, type, and size based on the requirements for your virtual appliance.
4. Power on and configure the virtual appliance.

Instructions for these procedures are provided in the following sections.

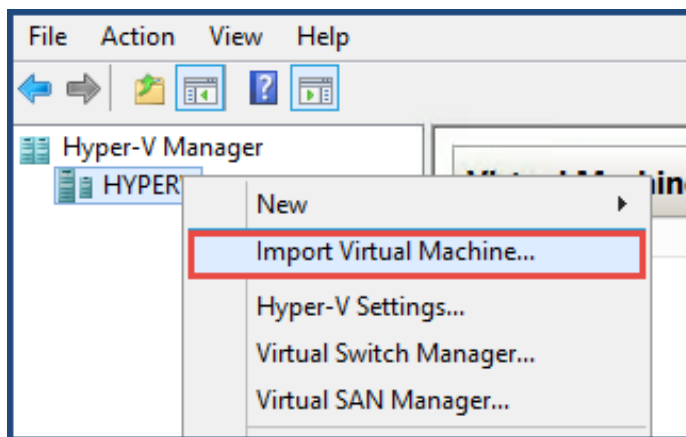
Importing the Virtual Machine

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

To import the virtual appliance:

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

Figure 27 Selecting the "Import Virtual Machine" Option

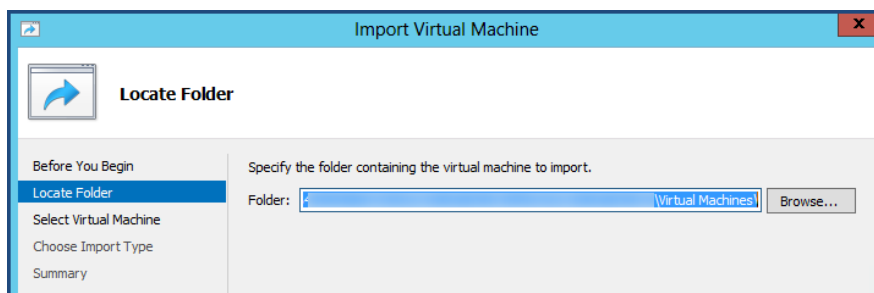


The **Before You Begin** dialog opens.

5. Click **Next**.

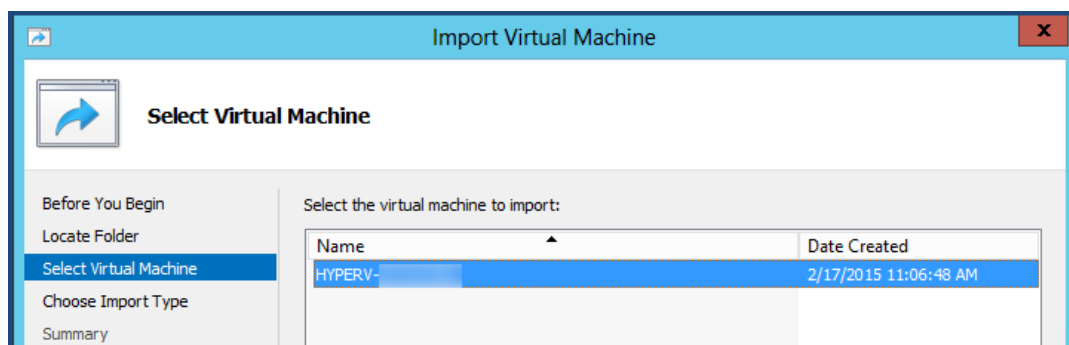
The **Locate Folder** dialog opens.

Figure 28 Locating the Folder



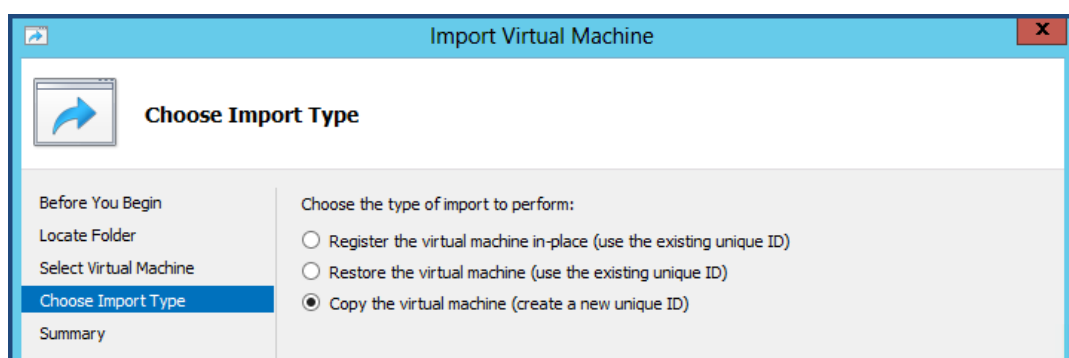
6. In the **Locate Folder** step, select the folder you unzipped in **Step 2**, then click **Next**.
The **Select Virtual Machine** dialog opens.

Figure 29 *Selecting the Virtual Machine*



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

Figure 30 *Specifying the Import Type*



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

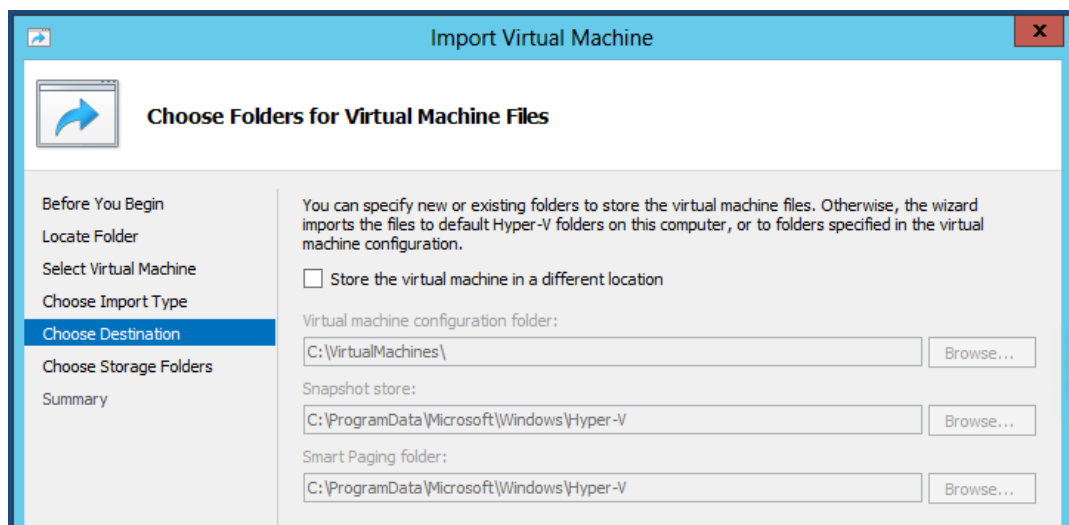


NOTE

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.

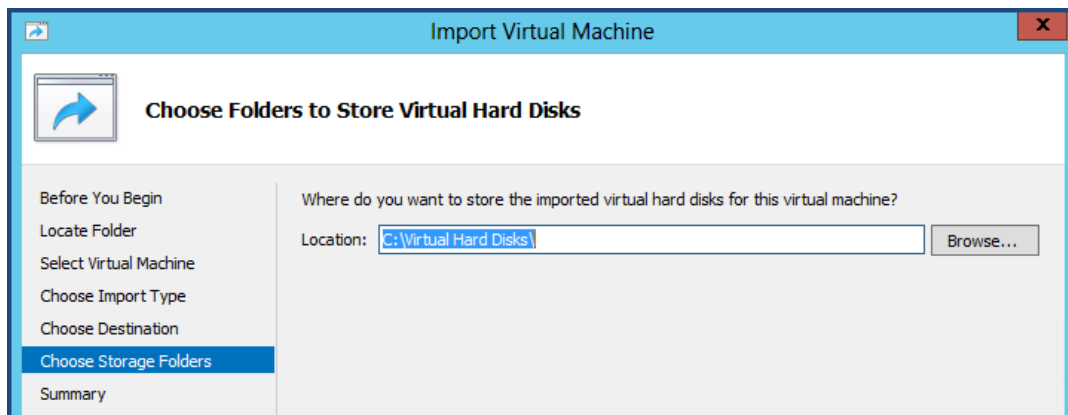
Figure 31 *Specifying the Folders for the Virtual Machine Files*



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

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

Figure 32 *Specifying Folders to Store Virtual Hard Disks*



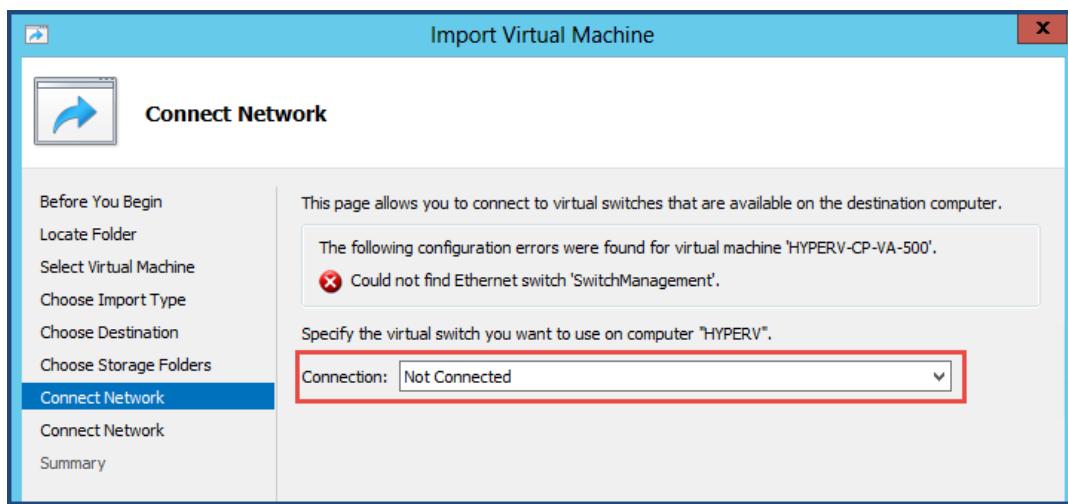
10. Accept the default virtual hard drive storage folder, or browse to a new location to change it to your preferred location, then click **Next**.



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

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

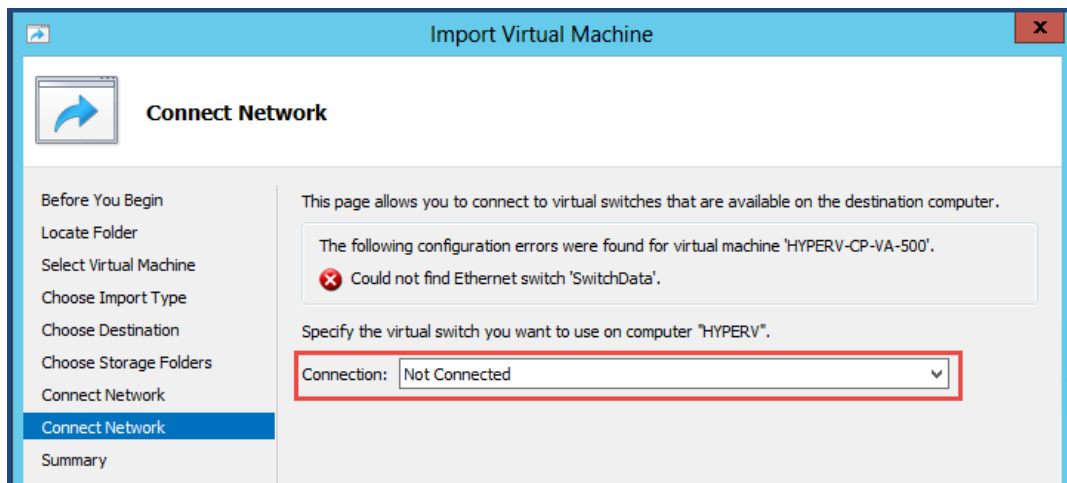
Figure 33 *Specifying the Virtual Switch in the Event of an Error*



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

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

Figure 34 *Specifying the Data Interface (Optional)*



12. You can choose to either specify the virtual switch that will be used for the Data interface or bypass this dialog.
 - a. To specify the virtual switch that will be used for the Data interface, from the **Connection** drop-down, choose the virtual switch that will be used for the Data interface, then click **Next**.
 - b. To bypass this configuration option, leave **Not connected** selected in the **Connection** drop-down, then click **Next**.

The **Completing Import Wizard** screen opens. This screen provides a summary of the import virtual appliance configuration that you specified.

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

This completes the procedure to import the virtual appliance.

Adding a Hard Disk to a Virtual Machine



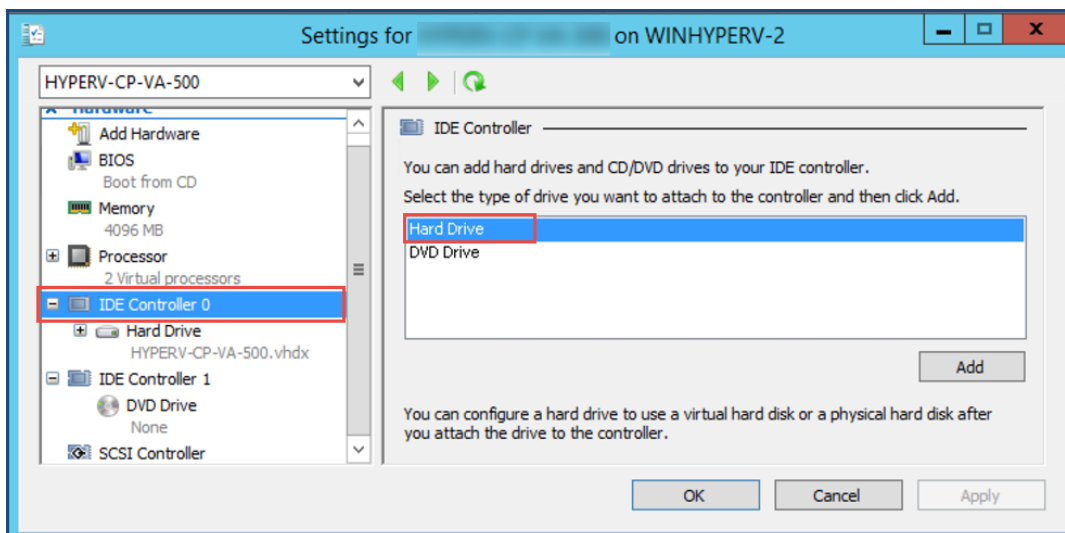
Do not create the virtual hard disk in a folder that is marked for encryption. Virtual hard disks are stored as .vhd files. Hyper-V does not support the use of storage media if Encrypting File System (EFS) has been used to encrypt the .vhd file. However, you can use files stored on a volume that uses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

To add a hard disk to a virtual machine:

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

The **Settings** page opens.

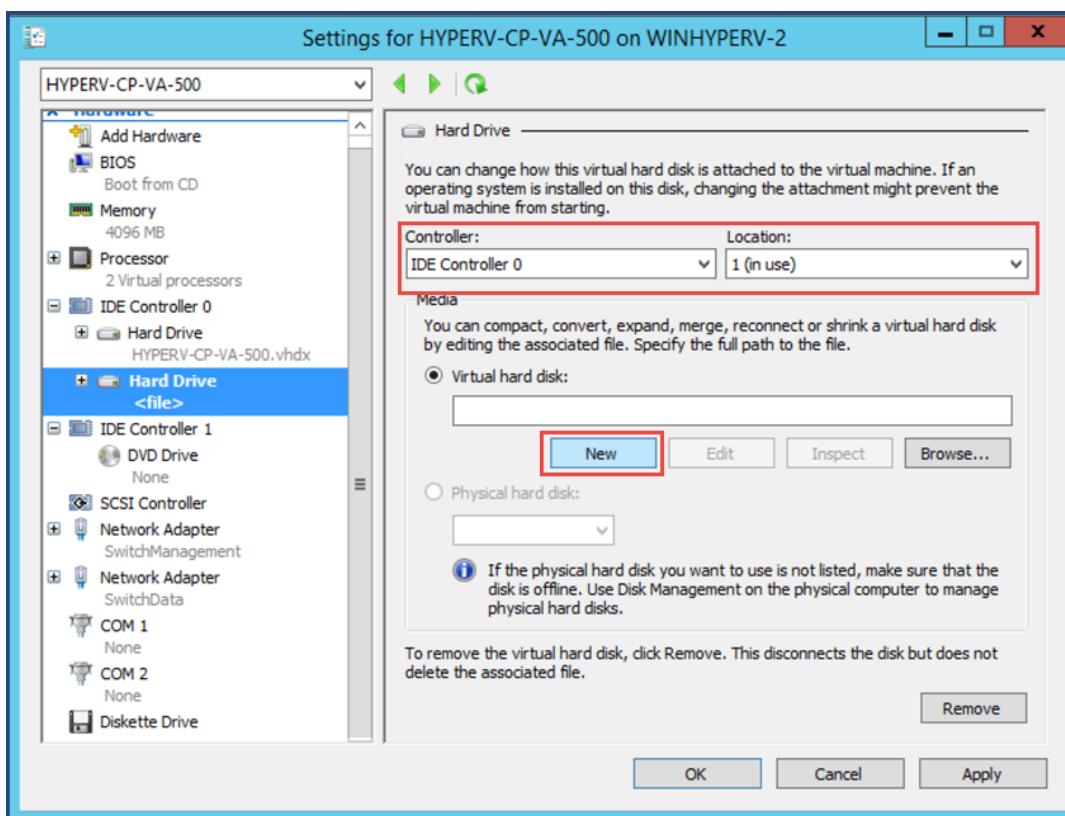
Figure 35 *Specifying the Controller*



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

The **Hard Drive** dialog opens.

Figure 36 *Configuring the Hard Drive*

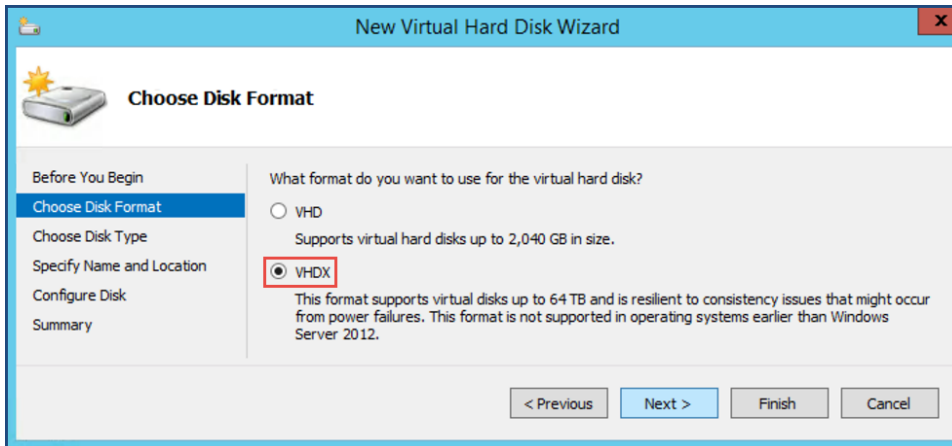


5. In the **Hard Drive** dialog:
 - a. **Controller**: Set to **IDE Controller 0**.
 - b. **Location**: Set to **1 (in use)**.
6. Below the **Virtual hard disk** field, click **New**.
The **New Virtual Hard Disk Wizard** opens.

7. From the **Before You Begin** dialog, click **Next**.

The **Choose Disk Format** dialog opens.

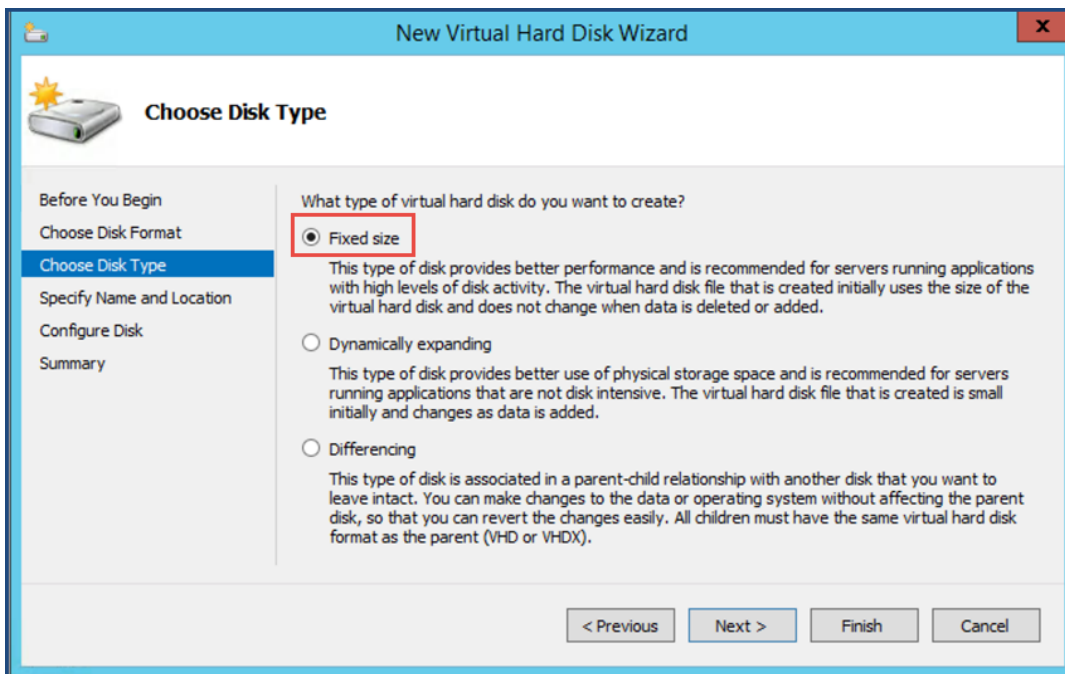
Figure 37 *Specifying the Disk Format*



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

The **Choose Disk Type** dialog opens.

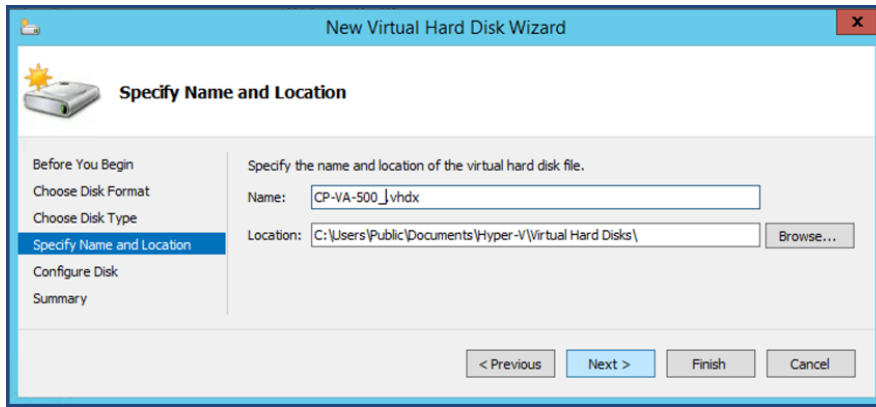
Figure 38 *Specifying the Virtual Hard Disk Type*



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

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

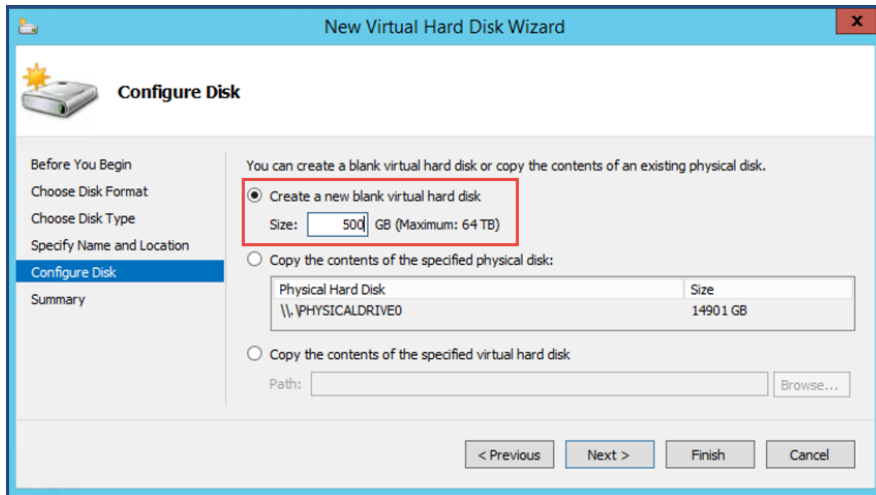
Figure 39 Specifying the Name and Location of the Hard Disk File



10. Do the following:

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

Figure 40 Configuring the New Virtual Hard Disk



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

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



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

- b. Click **Next**.

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

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

This completes the procedure to add a virtual hard disk.

Additional Virtual Hard Disk Considerations

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

- By default, membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure. However, an administrator can use Authorization Manager to modify the

authorization policy so that a user or group of users can complete this procedure.

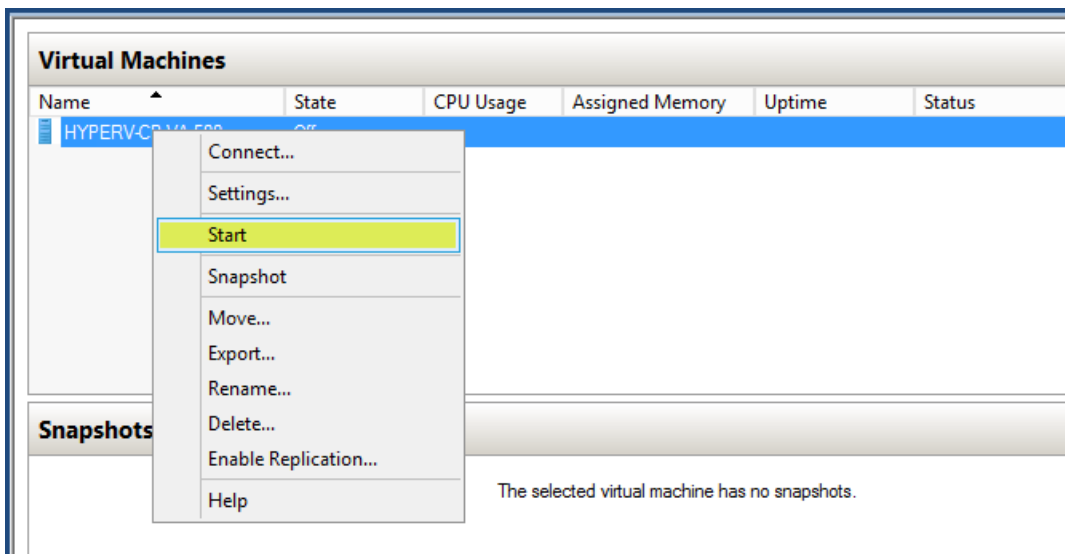
- Virtual hard disks are stored as .vhd files, which makes them portable, but it also poses a potential security risk. We recommend that you mitigate this risk by taking precautions such as storing the .vhd files in a secure location.
- The virtual hard disk is created when you click **Finish** to complete the wizard. Depending on the options you choose for the virtual hard disk, the process can take a considerable amount of time.
- Virtual hard disks cannot be stored in a folder that uses New Technology File System (NTFS) compression.
- You can make certain changes to a virtual hard disk after you create it. For example, you can convert it from one type of virtual hard disk to another. You can use the **Edit Virtual Hard Disk** wizard to make these changes.

Launching the ClearPass Virtual Appliance

To launch the ClearPass virtual appliance:

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

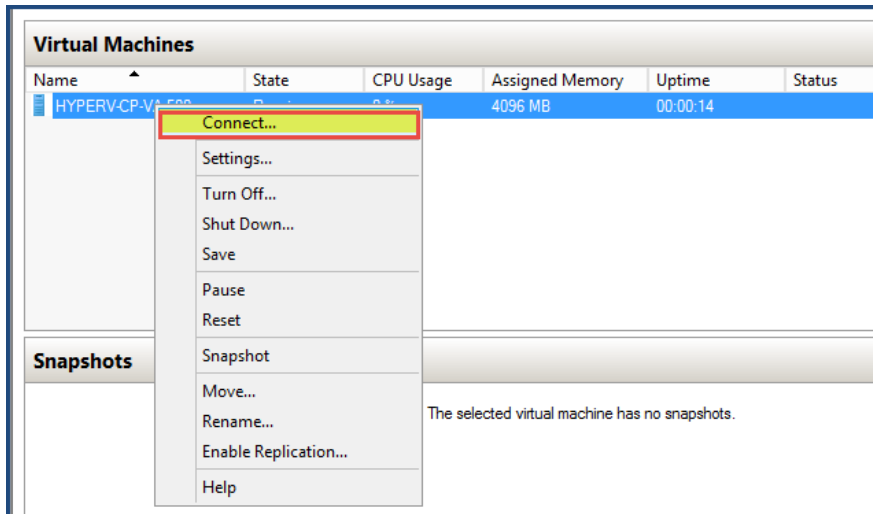
Figure 41 *Starting the Virtual Machine*



The virtual appliance powers on.

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

Figure 42 *Launching the VM Console*



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

Enter 'y' or 'Y' to proceed:

- To proceed with the installation, enter **y**.
ClearPass setup and installation begins.
The console screen appears.
- Enter the **number** for the appropriate appliance type (do not enter the appliance model itself).
For example, to specify the **C3000V** appliance, you would enter the number **4**. Options include:

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

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

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

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

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

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

Completing the Virtual Appliance Configuration

To complete the virtual appliance configuration:

- Refer to and note the required ClearPass server configuration information listed in [Table 8](#).
- Log in to the virtual appliance** using the following preconfigured credentials :
 - login: **appadmin**

- password: `<password>`

This initiates the Policy Manager Configuration wizard.

3. Configure the ClearPass virtual appliance.

Follow the prompts, replacing the placeholder entries in the following illustration with the information you entered in [Table 8](#).

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

4. Specify the cluster password.



Setting the cluster password also changes the password for the CLI user **appadmin**, as well as the Administration user **admin**. If you want the **admin** password to be unique, see [Changing the Administration Password on page 55](#).

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

5. Configure the system date and time.

- Follow the prompts to configure the system date and time.
- To set the date and time by configuring the NTP server, use the primary and secondary NTP server information you entered in [Table 8](#).

6. Apply the configuration.

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

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

Initial Login and Activation of the ClearPass Platform License

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

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

To specify the ClearPass Platform license upon initial login:

- After the configuration has been applied at the virtual appliance console, open a web browser and go to the management interface of ClearPass Policy Manager: **https://x.x.x.x/tips/**, where **x.x.x.x** is the IP address of the management interface defined for the ClearPass server in [Table 8](#).
- Log in to the ClearPass 6.7 server.

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

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

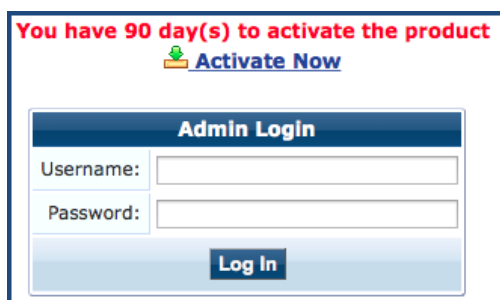
Figure 43 *Entering the ClearPass Platform License Key*

The screenshot shows the 'ClearPass Policy Manager' interface. At the top, a red banner reads 'To continue, please enter the product license key'. Below this, there is a 'Select Application' dropdown menu set to 'ClearPass Platform'. Underneath, the 'Enter license key' field contains 'APAA-'. A 'Terms and Conditions' section is visible, featuring the title 'Aruba Networks, Inc. End-User Software License Agreement ("Agreement")' and an 'IMPORTANT' notice. A checkbox labeled 'I agree to the above terms and conditions.' is checked. An 'Add License' button is located at the bottom right of the form.

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

Upon successfully entering the Platform License Key, the **Admin Login** screen appears with a message indicating that you have 90 days to activate the product and a link to activate the product.

Figure 44 *Activating ClearPass*

The screenshot displays the 'Admin Login' screen. At the top, a red banner states 'You have 90 day(s) to activate the product' with a green arrow icon and a link to 'Activate Now'. Below this, the 'Admin Login' section contains a 'Username:' field, a 'Password:' field, and a 'Log In' button.

7. To activate ClearPass on this virtual appliance, click **Activate Now**.
ClearPass Policy Manager attempts to activate the license over the Internet with Aruba license activation servers.
If the ClearPass Policy Manager virtual appliance does not have Internet access, you can perform the license activation offline by following the steps for offline activation presented in the **Offline Activation** section shown in [Figure 45](#).

Figure 45 *Activating the ClearPass Platform License*

Activate License

Online Activation
Activate Now

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

Step 1. Download an Activation Request Token **Download**

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

Step 3. **Browse...** No file selected. **Upload**

Upload the Activation Key received from Aruba Networks Support

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

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

Logging in to the ClearPass Virtual Appliance

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

Figure 46 *Logging in to the ClearPass Virtual Appliance*

Admin Login

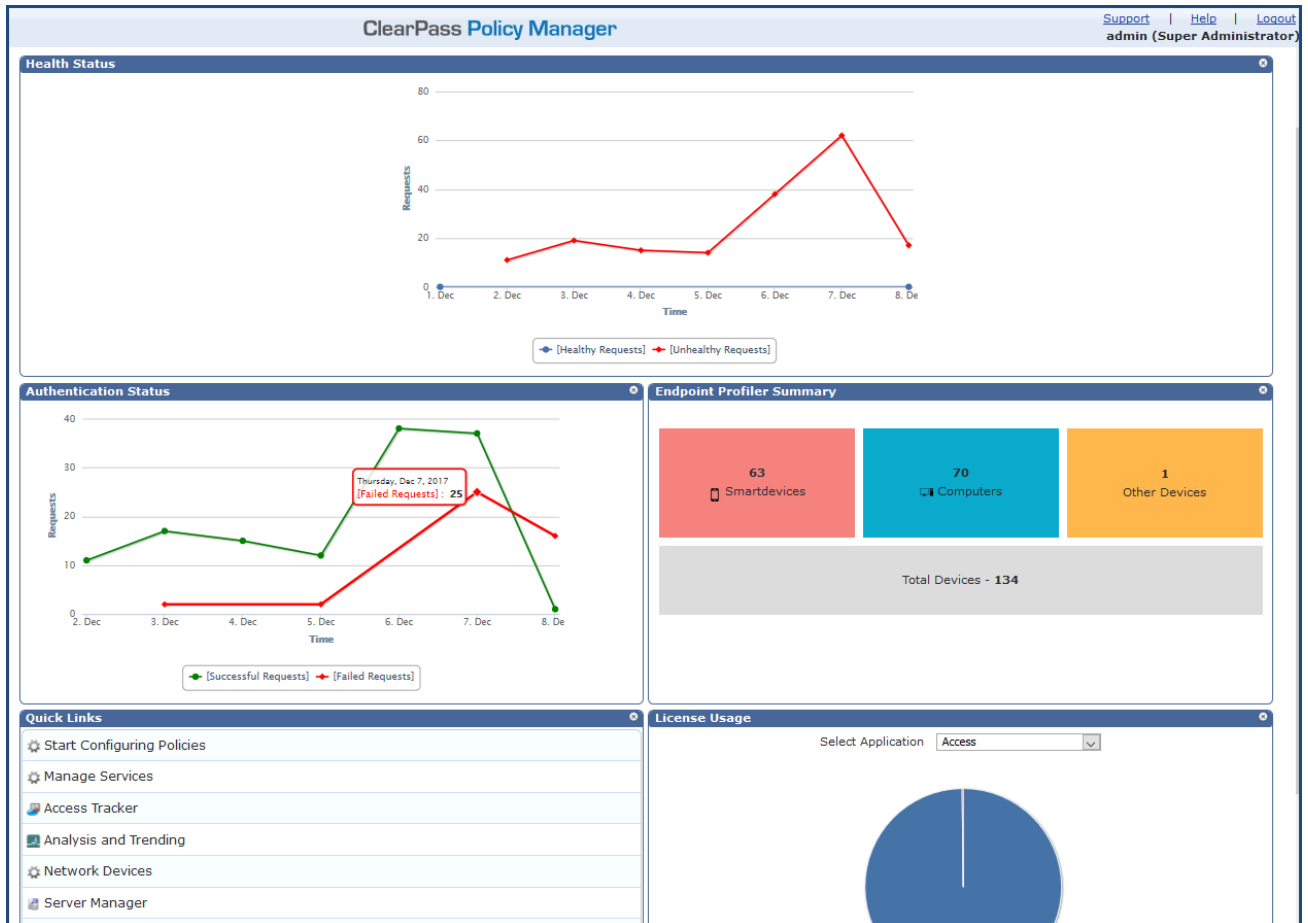
Username:

Password:

Log In

9. Log in to the ClearPass virtual appliance with the following credentials:
- **Username:** admin
 - **Password:** Enter the cluster password defined in [Completing the Virtual Appliance Configuration on page 48](#).
10. Click **Log In**.
The ClearPass Policy Manager Landing Page opens.

Figure 47 ClearPass Policy Manager Landing Page



About Software Updates

This section describes the ClearPass server software update process.

ClearPass checks for available updates to the ClearPass Webservice server. The administrator can download and install these updates directly from the **Software Updates** page (depending on the Cluster-Wide Parameter settings for those parameters). Use the **Software Updates** page to configure and receive live updates for:

- **Posture Signature updates**

These updates include AntiVirus version updates. The ClearPass server uses these updates to check if the versions of the AntiVirus and the DAT file are the latest version.

- **Windows Hotfixes updates**

These updates include a list of available Windows Hotfixes for supported Windows operating systems. The ClearPass server uses these updates to show a list of the available hotfixes in the Windows Hotfixes health class.

- **Endpoint Profile Fingerprints updates**

These updates include fingerprints and are used by ClearPass in profiling endpoints.



Automatic download and installation for these three types of updates are not enabled by default.

You can also:

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

- Uninstall a skin.

Software Updates Page

To update the software on the current ClearPass server:

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

[Figure 48](#) displays the **Software Updates** page:

Figure 48 *Software Updates Page*

Administration » Agents and Software Updates » Software Updates

Software Updates

Cluster Upgrade
Cluster Update
Check Status Now

HPE Passport Credentials

Username:

Password:

Save

Posture & Profile Data Updates

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

Import Updates

* Automatic download and install is disabled
To manually import Posture & Profile Data Updates, refer to Help for this page.

Firmware & Patch Updates

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

Import Updates

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

Check Status Now

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

Table 9: *Software Updates Page Parameters*

Parameter	Action/Description
HPE Passport Credentials	
HPE Passport Credentials	<p>Enter the HPE Passport Credentials provided to you.</p> <p>This text box is enabled only on a Publisher node.</p> <p>The first time the HPE Passport Credentials are saved, the ClearPass server performs the following operations:</p> <ul style="list-style-type: none"> • Contacts the Webservice server to download the latest Posture & Profile Data updates (depending on the Cluster-Wide Parameter settings for those parameters). • Checks for any available firmware and patch updates.
Posture & Profile Data Updates	

Parameter	Action/Description
Import Updates	<p>To download the Posture and Profile Data Updates to the client (for example, a Windows laptop):</p> <ol style="list-style-type: none"> 1. From the client device, log in to the Aruba Support Center. 2. Select the Download Software tab, then navigate to ClearPass > Tools > Posture & Profile Data Updates. 3. Click the desired update(s) (which are in zip file format) and save the file. 4. From ClearPass, click the Posture and Profile Data Updates > Import Updates button to import the downloaded file into ClearPass. <p>NOTE: In a ClearPass cluster, the Import Updates option is available on the Publisher node only.</p> <p>By default, updates for Posture Signature, Windows Hotfixes, and Endpoint Profile Fingerprints are <i>not</i> automatically downloaded and installed. To set these updates to be automatic, you must set the following <i>Cluster-Wide Parameters</i> to TRUE:</p> <ul style="list-style-type: none"> • Automatically download Posture Signature and Windows Hotfixes Updates • Automatically download Endpoint Profile Fingerprints
<p>Firmware & Patch Updates</p> <p>NOTE: The Firmware & Patch Updates table shows only the data that is known to Webservice or imported using the Import Updates button.</p> <p>NOTE: Patch residual files under <i>/var/avenda/platform/backup</i>, <i>/var/avenda/platform/patches</i>, and <i>/var/avenda/platform/store/updates</i> seven days old and older are automatically deleted daily.</p>	
Import Updates	<p>If the server is not able to reach the Webservice server, click Import Updates to import the latest signed Firmware and Update patch binaries (obtained via support or other means) into this server.</p> <p>These patch binaries will appear in the table and can be installed by clicking the Install button. When logged in as <i>appadmin</i>, you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands:</p> <ul style="list-style-type: none"> • system update (for patches) • system upgrade (for upgrades) <p>If a patch requires a prerequisite patch, that patch's Install button will not be enabled until the prerequisite patch is installed.</p>
Install	<p>The Install button appears after the update has been downloaded.</p> <p>Click Install.</p> <p>When you click Install, the installation of the update starts and the Install Update dialog box appears, showing the log messages that are generated.</p>
Re-Install	<p>Click Re-Install to reinstall a patch in the event the previous attempt to install fails.</p> <p>Reinstalling a patch is available only for the last installed patch.</p>

Parameter	Action/Description
Uninstall	To uninstall a skin, click Uninstall (for details, see Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance). NOTE: You cannot uninstall cumulative or point patch updates.
Needs Restart	The Needs Restart link appears when an update needs a reboot of the server in order to complete the installation. Clicking this link displays the Install Update dialog box, which shows the log messages generated during the installation.
Installed	The Installed link appears when an update has been successfully installed. Clicking this link displays the Install Update dialog box, which shows the log messages generated during the installation.
Install Error	This link appears when an update install encounters an error. Clicking this link displays the Install Update dialog box, which shows the log messages generated during the install.
Other	
Check Status Now	Click this button to perform an on-demand check for available updates. Check Status Now applies to updates only on a Publisher node, as well as Firmware & Patch Updates.
Delete	Use this option to delete a downloaded update.

Changing the Administration Password

When the cluster password for this ClearPass server is set upon initial configuration (see [Completing the Virtual Appliance Configuration on page 48](#)), the administration password is also set to the same password. If you wish to assign a unique **admin** password, use this procedure to change it.

To change the administration password:

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

The **Admin Users** page opens.

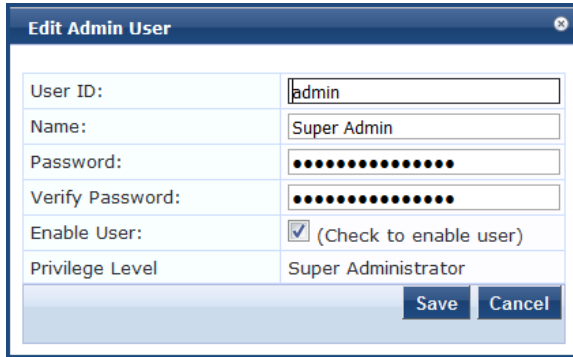
Figure 49 Admin Users Page

Administration » Users and Privileges » Admin Users				
Admin Users				
<div> Add Import Export All Account Settings </div>				
Filter: User ID <input type="text"/> contains <input type="text"/> <input type="button" value="Go"/> <input type="button" value="Clear Filter"/> Show 10 records				
#	<input type="checkbox"/> User ID ▲	Name	Privilege Level	Status
1.	<input checked="" type="checkbox"/> admin	Super Admin	Super Administrator	Enabled
2.	<input type="checkbox"/> apiadmin	API Admin	API Administrator	Enabled
Showing 1-2 of 2				<input type="button" value="Export"/> <input type="button" value="Delete"/>

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

The **Edit Admin User** dialog opens.

Figure 50 *Changing the Administration Password*



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

Save Cancel

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

Powering Off the ClearPass Virtual Appliance

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

To power off the ClearPass virtual appliance:

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

The ClearPass virtual appliance shuts down.

Maintaining ClearPass Policy Manager Services

This section contains the following information:

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

Starting or Stopping ClearPass Services

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

To access the **Services Control** page:

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

Figure 51 ClearPass Server Configuration Page for Selected Server

Administration » Server Manager » Server Configuration - 51.120
Server Configuration - 51.120 (10.)

System Services Control Service Parameters System Monitoring Network FIPS

Hostname: 51.120

FQDN:

Policy Manager Zone: default [Manage Policy Manager Zones](#)

Enable Performance Monitoring Display: ☒ Enable this server for performance monitoring display

Insight Setting: ☐ Enable Insight

Enable Ingress Events Processing: ☐ Enable Ingress Events processing on this server

Master Server in Zone: Primary master

Span Port: -- None --

	IPv4	IPv6	Action
Management Port	IP Address	10.	Configure
	Subnet Mask	255.255.255.0	
	Default Gateway	10.	
Data/External Port	IP Address	192.168.168.13	Configure
	Subnet Mask	255.255.255.0	
	Default Gateway	192.	
DNS Settings	Primary	10.1.10.10	Configure
	Secondary	10.2.10.10	
	Tertiary		
	DNS Caching	Disabled	

AD Domains: Policy Manager is not part of any domain. Join to domain here. [Join AD Domain](#)

3. Select the **Services Control** tab.
The **Services Control** page opens.

Figure 52 *Server Configuration > Services Control Page*

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

[Back to Server Configuration](#) Save Cancel



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

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

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

Starting Services from the Command Line

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

```
service start <service_name>
```

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

```
service start all
```

Summary of the Server Configuration Page

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

[Table 10](#) describes each of the top-level server configuration options that are available. For details, refer to the "Server Configuration" section in the "Administration" chapter of the *ClearPass Policy Manager User Guide*.

Table 10: *Description of the Server Configuration Page*

Tab	Description	Comments
System	Displays server identity and connection parameters. The configurations for the management port and the data port are also displayed.	This tab also provides parameters to allow you to enable Insight and specify the Insight master, enable OnConnect, and enable ingress events processing.
Services Control	You can view the status of a Policy Manager service (that is, see whether a service is running or not), and stop or start services.	
Service Parameters	This option allows you to change the system parameters for all services.	The options on this page vary based on the service selected.
System Monitoring	This option allows you to configure SNMP parameters, ensuring that external MIB browsers can browse the system-level MIB objects exposed by the Policy Manager appliance.	The options on this page vary based on the SNMP version that you select.
Network	Use the Network page to: <ul style="list-style-type: none"> • Configure Application Access Control—allow or deny access to network resources. • Add SSH Public Keys • Create generic routing encapsulation (GRE) tunnels • Create IPsec tunnels • Create VLANs related to guest users. 	<ul style="list-style-type: none"> • A GRE tunnel creates a virtual point-to-point link between controllers over a standard IP network or the Internet. • To create VLANs, your network infrastructure must support tagged 802.1Q packets on the physical interface selected.
FIPS	Enables 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 ClearPass Maintenance Tasks

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

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

```
*****
* Policy Manager CLI v6.7(0), Copyright © 2017, Aruba Networks, an HPE Company
*
* Software Version : 6.7.0 062080
*****

Logged in as group Local Administrator
[appadmin@company.com] #
```

CLI Task Examples

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

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

Reconfigure DNS or Add a New DNS

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

Reconfigure or Add Management and Data Ports

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

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

Configure the Date

Configuring the time and time zone is optional.

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

Configure the Host Name for the Node

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

Join the ClearPass Policy Manager Appliance to the Active Directory Domain

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

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

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

Copyright

© Copyright 2018 Hewlett Packard Enterprise Development LP

All rights reserved. Specifications in this manual are subject to change without notice.

Originated in the USA. All other trademarks are the property of their respective owners.

Open Source Code

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

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

© Copyright 2017 Hewlett Packard Enterprise Development LP



www.arubanetworks.com

3333 Scott Blvd

Santa Clara, California 95054

Phone: 408.227.4500