ClearPass Getting Started Guide
Copyright Information

© Copyright 2017 Hewlett Packard Enterprise Development LP.

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

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

Open Source Code

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

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

Please specify the product and version for which you are requesting source code.
Contents

Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance ...........................................35
Introduction ........................................................................................................................................35
Before Starting the ClearPass Installation .........................................................................................36
ClearPass Hyper-V Virtual Appliance Installation Summary ..........................................................37
Importing the Virtual Machine .............................................................................................................37
Adding a Hard Disk to a Virtual Machine ..........................................................................................41
Launching the ClearPass Virtual Appliance .......................................................................................45
Completing the Virtual Appliance Configuration .............................................................................48
Applying and Activating the ClearPass License ...............................................................................49
Logging in to the ClearPass Virtual Appliance ................................................................................50
Signing Up for Live Software Updates ..............................................................................................51
Changing the Administration Password ............................................................................................52
Powering Off the ClearPass Virtual Appliance ..................................................................................52
Maintaining ClearPass Services ......................................................................................................53
Maintaining ClearPass Policy Manager Services ..............................................................................53
Starting or Stopping ClearPass Services ............................................................................................53
Summary of the Server Configuration Page .......................................................................................54
Subset of CLI for ClearPass Maintenance Tasks ...............................................................................54
This chapter documents the procedures for installing and configuring ClearPass on a hardware appliance.

About This Guide

Welcome to the *ClearPass 6.7 Getting Started Guide*. This guide contains the following information:

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

Intended Audience

The intended audience for the *ClearPass 6.7 Getting Started Guide* includes customers, partners, system administrators, and Aruba/HP Enterprise field System Engineers.

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

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

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

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

About the ClearPass Access Management System

This section contains the following information:

- ClearPass Access Management System Overview
- Key Features
- Advanced Policy Management
- ClearPass Policy Manager Hardware and Virtual Appliances
- ClearPass Specifications

ClearPass Access Management System Overview

The 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 multi-vendor 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 workflows that previously required manual IT intervention. It integrates with mobile device management to leverage device inventory and posture information, which enables better-informed policy decisions.

Key Features

ClearPass's key features are as follows:

- Role-based network access enforcement for multivendor Wi-Fi, wired, and VPN networks
- High performance, scalability, High Availability, and load balancing
- A Web-based user interface that simplifies policy configuration and troubleshooting
- Network Access Control (NAC), Network Access Protection (NAP) posture and health checks, and Mobile Device Management (MDM) integration for mobile device posture checks
- Auto Sign-On and single sign-on (SSO) support via Security Assertion Markup Language (SAML) v2.0
- Social Network and Cloud Application SSO via OAuth2
  - Facebook, Twitter, LinkedIn, Office365, Google Apps, and so on
- Built-in Bring Your Own Device (BYOD) Certificate Authority for secure self-service onboarding
- Advanced reporting of all user authentications and failures
- Enterprise Reporting, Monitoring, and Alerting
- HTTP/RESTful APIs for integration with third-party systems, Internet security, and Mobile Device Management (MDM)
- Device profiling and self-service onboarding
- Guest access with extensive branding and customization and sponsor-based approvals
- IPv6 administration support
Advanced Policy Management

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

- **Customizable visitor management**
  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, perform advanced endpoint posture assessments. Traditional NAC health-check capabilities ensure compliance and network safeguards before devices connect.
  You can use information about endpoint integrity (such as status of anti-virus, anti-spyware, firewall, and peer-to-peer applications) to enhance authorization policies. Automatic remediation services are also available for non-compliant devices.

**ClearPass Policy Manager Hardware and Virtual Appliances**

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

To increase scalability and redundancy, you can deploy virtual appliances, as well as the hardware appliances, within a cluster.
• For ClearPass hardware appliance installation and deployment procedures, see Setting Up the ClearPass Hardware Appliances on page 9.

• For ClearPass virtual appliance installation and deployment procedures:
  ■ VMware ESX and ESXi: Using VMware vSphere Web Client to Install ClearPass on a Virtual Machine on page 21
  ■ Microsoft Hyper-V: Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance on page 35.

ClearPass Specifications

ClearPass Policy Manager
• Comprehensive identity-based policy engine
• Posture agents for Windows, Mac OS X, and Linux operating systems
• Built-in AAA services: RADIUS, TACACS+, and Kerberos
• Web, 802.1X, and non-802.1X authentication and authorization
• Reporting, analytics, and troubleshooting tools
• External captive portal redirect to multivendor equipment
• Interactive policy simulation and monitor mode utilities
• Deployment templates for any network type, identity store, and endpoint

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

Supported Identity Stores
• Microsoft Active Directory
• Kerberos
• Any LDAP-compliant directory
• Any ODBC-compliant SQL server
• Token servers
• Built-in SQL store
• Built-in static-hosts list
Setting Up the 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 provides the following information:
- About the ClearPass Hardware Appliances
- ClearPass Policy Manager 500 Hardware Appliance
- ClearPass Policy Manager 5K Hardware Appliance
- ClearPass Policy Manager 25K Hardware Appliance
- Before Starting the ClearPass Installation
- Configuring the ClearPass Hardware Appliance
- Activating ClearPass
- Logging in to the ClearPass Hardware Appliance
- Signing Up for Live Software Updates
- 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 500: See ClearPass Policy Manager 500 Hardware Appliance
- ClearPass Policy Manager 5K: See ClearPass Policy Manager 5K Hardware Appliance.

<table>
<thead>
<tr>
<th>Table 1: Functional Description of the ClearPass Hardware Appliance Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong></td>
</tr>
<tr>
<td>Serial port</td>
</tr>
<tr>
<td>VGA connector</td>
</tr>
<tr>
<td>USB ports</td>
</tr>
<tr>
<td>Management port (Gigabit Ethernet)</td>
</tr>
<tr>
<td>Data port (Gigabit Ethernet)</td>
</tr>
<tr>
<td>iDRAC7 Enterprise port</td>
</tr>
</tbody>
</table>
ClearPass Policy Manager 500 Hardware Appliance

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

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

Figure 1 shows the ports on the rear panel of the ClearPass 500 hardware appliance. The function of each of these ports is described in Table 1.

Figure 1: Ports on the ClearPass 500 Hardware Appliance

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

Table 2 describes the specifications for the ClearPass Policy Manager 500 hardware appliance.

Table 2: CP-HW-500 Specifications

<table>
<thead>
<tr>
<th>CP-HW-500 Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Pentium G850, Dual Core, 2.9Ghz, 3 MB Cache</td>
</tr>
<tr>
<td>Memory</td>
<td>4 GB (2 x2 GB)</td>
</tr>
<tr>
<td>Hard drive storage</td>
<td>500 GB 7.3 K RPM, Serial ATA</td>
</tr>
<tr>
<td>Maximum unique endpoints</td>
<td>• High Capacity Guest (HGC) mode enabled: 1,000</td>
</tr>
<tr>
<td></td>
<td>• HGC not enabled: 500</td>
</tr>
<tr>
<td>Maximum number of authentications per day</td>
<td>• High Capacity Guest (HGC) mode enabled: 40,000</td>
</tr>
<tr>
<td></td>
<td>• HGC not enabled: 20,000</td>
</tr>
<tr>
<td>Form Factor</td>
<td></td>
</tr>
<tr>
<td>Dimensions (WxHxD)</td>
<td>16.8&quot; x 1.7&quot; x 14&quot;</td>
</tr>
<tr>
<td>Weight (max configuration)</td>
<td>14 lbs</td>
</tr>
<tr>
<td>Power Specifications</td>
<td></td>
</tr>
<tr>
<td>Power consumption (maximum)</td>
<td>260 watts</td>
</tr>
<tr>
<td>Power supply</td>
<td>Single</td>
</tr>
<tr>
<td>AC input voltage</td>
<td>100/240 VAC auto-selecting</td>
</tr>
<tr>
<td>AC input frequency</td>
<td>50/60 Hz auto-selecting</td>
</tr>
</tbody>
</table>
### CP-HW-500 Component Specification

#### Environmental Specifications

<table>
<thead>
<tr>
<th>Specification</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating temperature</td>
<td>10°C to 35°C (50°F to 95°F)</td>
</tr>
<tr>
<td>Operating vibration</td>
<td>0.26 G at 5 Hz to 350 Hz for 5 minutes</td>
</tr>
<tr>
<td>Operating shock</td>
<td>1 shock pulse of 31 G for up to 2.6 ms</td>
</tr>
<tr>
<td>Operating altitude</td>
<td>-16 m to 3,048 m (-50 ft to 10,000 ft)</td>
</tr>
</tbody>
</table>

### ClearPass Policy Manager 5K Hardware Appliance

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

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

Figure 2 shows the ports on the rear panel of the ClearPass Policy Manager 5K hardware appliance. The function of each of these ports is described in Table 1.

**Figure 2: Ports on the ClearPass 5K Hardware Appliance**

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

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

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

<table>
<thead>
<tr>
<th>CP-HW- 5K Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Xeon E3-1220 3.10 GHz, 8 M Cache, Quad Core/4T</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB Memory (4 x 2 GB)</td>
</tr>
<tr>
<td>Hard disks</td>
<td>(2) 1 TB 7.2K RPM SATA 3 Gbps</td>
</tr>
<tr>
<td>RAID controller</td>
<td>PERC H200</td>
</tr>
<tr>
<td>RAID configuration</td>
<td>1</td>
</tr>
<tr>
<td>OOB management</td>
<td>Baseboard Management Controller (BMC)</td>
</tr>
<tr>
<td>Maximum unique endpoints</td>
<td>High Capacity Guest (HGC) mode enabled: 10,000</td>
</tr>
<tr>
<td>CP-HW-5K Component</td>
<td>Specification</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>- HGC not enabled: 5,000</td>
<td></td>
</tr>
</tbody>
</table>
| Maximum number of authentications per day | - High Capacity Guest (HGC) mode enabled: 400,000  
- HGC not enabled: 200,000 |

**Form Factor**

- Dimensions (WxHxD): 17.53” x 1.7” x 16.8”
- Weight (max configuration): 18 lbs

**Power Specifications**

- Power consumption (maximum): 250 watts
- Power supply: Single
- AC input voltage: 100/240 VAC auto-selecting
- AC input frequency: 50/60 Hz auto-selecting

**Environmental Specifications**

- Operating temperature: 10º C to 35º C (50º F to 95º F)
- Operating vibration: 0.26 G at 5 Hz to 350 Hz for 5 minutes
- Operating shock: 1 shock pulse of 31 G for up to 2.6 ms
- Operating altitude: -16 m to 3,048 m (-50 ft to 10,000 ft)

**ClearPass Policy Manager 25K Hardware Appliance**

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

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

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

Figure 3 shows the ports on the rear panel of the ClearPass 25K hardware appliance.

**Figure 3: Ports on the ClearPass 25K Hardware Appliance**
Table 4 describes the specifications for the ClearPass Policy Manager 25K hardware appliance.

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

<table>
<thead>
<tr>
<th>CP-HW-25K Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPUs</td>
<td>(2) Xeon X5650 2.66 Ghz, 12 M Cache, Turbo, HT</td>
</tr>
<tr>
<td>Memory</td>
<td>48 GB Memory (12 x 4 GB)</td>
</tr>
<tr>
<td>Hard disks</td>
<td>(4) 300 GB 10 K RPM Serial-Attach SCSI 6 Gbps</td>
</tr>
</tbody>
</table>
| Maximum unique endpoints | ● High Capacity Guest (HGC) mode enabled: 50,000  
● HGC not enabled: 25,000 |
| Maximum number of authentications per day | ● High Capacity Guest (HGC) mode enabled: 2 million  
● HGC not enabled: 1 million |
| RAID controller     | ● PERC 6/i  
| RAID configuration  | ● 10 |
| OOB management      | iDRAC7 Enterprise |

**Form Factor**

| Dimensions (WxHxD) | 16.8” x 1.7” x 27.8” |
| Weight (max configuration) | Up to 39 lbs |

**Power Specifications**

| Power consumption (maximum) | 750 watts |
| Power supply               | Dual hot-swappable (optional) |
| AC input voltage           | 100/240 VAC auto-selecting |
| AC input frequency         | 50/60 Hz auto-selecting |

**Environmental Specifications**

| Operating temperature | 10° C to 35° C (50° F to 95° F) |
| Operating vibration     | 0.26 G at 5 Hz to 350 Hz for 5 minutes |
| Operating shock         | 1 shock pulse of 31 G for up to 2.6 ms |
| Operating altitude      | -16 m to 3,048 m (-50 ft to 10,000 ft) |
Before Starting the 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 Values

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

Configuring the ClearPass Hardware Appliance

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

To configure the ClearPass Policy Manager hardware appliance:

1. **Connect the Serial port.**
   a. Connect the Serial port to a terminal using the null modem cable provided.
   b. Power on the hardware appliance.
      The hardware appliance is now available for configuration.

2. **Configure the Serial port.**
   Apply the following parameters for the Serial port:
   - **Bit Rate:** 9600
   - **Data Bits:** 8
   - **Parity:** None
   - **Stop Bits:** 1
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.

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

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

   a. Follow the prompts to configure the system date and time.
   b. To set the date and time by configuring the NTP server, use the primary and secondary NTP server information you entered in Table 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 ClearPass Policy Manager.

### 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 go to the ClearPass Policy Manager management interface:

   ```
   https://x.x.x.x/tips/
   ```

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

   ![Activating ClearPass](image)

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 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**

   ![Performing Offline Activation](image)

   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 Hardware Appliance

After a successful activation, the Admin Login dialog opens.

Figure 6: Logging in to the ClearPass Hardware Appliance

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 home page is displayed.

Figure 7: ClearPass Policy Manager Home Page

Signing Up for Live Software Updates

Upon your initial login to ClearPass Policy Manager, register for software updates.

1. Navigate to the Administration > Agents and Software Updates > Software Updates page.
   A message is displayed indicating that the ClearPass hardware appliance is not signed up for live updates and that you must enter your subscription ID.
2. If the ClearPass Policy Manager server has Internet access, enter your subscription ID, then click Save.
   After successfully applying the subscription ID, you will see a message indicating that the subscription ID was updated successfully and ClearPass is processing updates from the ClearPass Webservice.
   Note that Posture & Profile Data Updates are downloaded and installed automatically, while Firmware & Patch Updates are displayed only.

**Changing the Administration Password**

When the cluster password for this 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 appears.

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

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

Generating the Password Recovery Key

To generate the password recovery key:
1. If you are employing a hardware connection, connect to the 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 vSphere console (see Using VMware vSphere Web Client to Install ClearPass on a Virtual Machine on page 21) or the Hyper-V hypervisor (Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance on page 35).
2. Reboot the system using the restart command.
3. After the system reboots, the following prompt is displayed for ten seconds:
   
   Generate support keys? [y/n]:

4. At the prompt, enter y.

The system prompts you with the following choices:

   Please select a support key generation option.
   1) Generate password recovery key
   2) Generate a support key
   3) Generate password recovery and support keys

   Enter the option or press any key to quit.

5. To generate a password recovery key, select option 1.
6. After the password recovery key is generated, open a support case with Aruba Technical Support

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

Resetting the System Account Passwords to the Factory Defaults

To reset the administrator password:
1. Log in as the apprecovery user with the password recovery key provided by Aruba Technical Support.
2. Enter the following command at the command prompt:
   
   [apprecovery] app reset-pwd

   *******************************************************
* WARNING: This command will reset the system account *
* passwords to factory default values                      *
******************************************************************************

Are you sure you want to continue? [y/n]: y
INFO - Password changed on local node
INFO - System account passwords have been reset to factory default values

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

4. You can now log in with the new administrator password sent to you by Aruba Technical Support.
Chapter 2
Setting Up ClearPass Virtual Machines

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

This chapter includes the following information:
- Using VMware vSphere Web Client to Install ClearPass on a Virtual Machine
- Using Microsoft Hyper-V to Install ClearPass on a Virtual Appliance

Using VMware vSphere 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 an 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
- 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
- Applying and Activating the ClearPass License
- Logging in to the ClearPass Virtual Appliance
- Signing Up for Live Software Updates
- 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 ESX/ESXi Server Specifications

Carefully review all virtual appliance requirements, including functional IOP ratings, and verify that your system meets these requirements. These recommendations supersede earlier requirements that were published for ClearPass Policy Manager 6.x 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 ClearPass virtual appliance.
Supplemental Storage/Hard Disk Requirement

All VMware ESXi virtual machines use hardware version 8.

ClearPass VMware ships with a 20 GB hard disk volume. This must be supplemented with additional storage/hard disk by adding a virtual hard disk (see Adding a Virtual Hard Disk on page 26 for details). The additional space required depends on the 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 appropriate version folders under Aruba Support Center > Documentation > Software User & Reference Guides > ClearPass > Release Notes.

Supported Hypervisors

ClearPass supports the following ESX hypervisors:

- VMware ESXi versions 5.0, 5.1, 5.5, 6.0, and higher

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

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Value for Your Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name (Policy Manager server)</td>
<td></td>
</tr>
<tr>
<td>Management interface IP address</td>
<td></td>
</tr>
<tr>
<td>Management interface subnet mask</td>
<td></td>
</tr>
<tr>
<td>Management interface gateway</td>
<td></td>
</tr>
<tr>
<td>Data port IP address (optional)</td>
<td></td>
</tr>
<tr>
<td>Data interface subnet mask (optional)</td>
<td><strong>NOTE:</strong> Make sure that the Data interface IP address is <em>not</em> in the same subnet as the Management interface IP address.</td>
</tr>
</tbody>
</table>
### Required Information

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Value for Your Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data interface gateway (optional)</td>
<td></td>
</tr>
<tr>
<td>Primary DNS</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS</td>
<td></td>
</tr>
<tr>
<td>NTP server (optional)</td>
<td></td>
</tr>
</tbody>
</table>

### vSphere Web Client ClearPass Installation Overview

ClearPass 6.x 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:

2. To extract the files, unzip the files to a folder on your server.
3. Follow the steps in the OVF wizard to deploy the OVF file, **but do not power on yet**.

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

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

### 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.
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 2 and Step 3**.

The Deploy OVF Template appears.

If you are not using the vSphere Web Client or the standard vSphere Client, follow the instructions for your method of deploying the OVF file.
Figure 11: Deploy OVF Template: Selecting the Source Location

6. Select Local File, then click **Browse**.

7. Navigate to the folder where you extracted the files, then click **Next**.
   The *Review Details* screen opens.

8. Review the information presented, then click **Next**.
   The *Accept EULAs* screen opens.

9. Read the End User License Agreements (EULA) and click **Accept**, then click **Next**.
   The *Select Name and Folder* screen opens.

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

10. In the *Select Name and Folder* dialog:
    The name of the template is set by default to *Aruba 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 13: Selecting a Resource

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

Figure 14: Selecting the Location to Store the Files

12. Choose the virtual disk format and data store for the ClearPass virtual appliance, then click Next.
   The virtual disk format specified in Figure 14 is Thin Provision. In a production environment, to ensure that the virtual appliance will not run out of disk space, Aruba recommends using the Thick Lazy Zeroed virtual disk format.

The Setup Networks screen opens.

Figure 15: Configuring the Networks for VM Deployment

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

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

14. Review the settings for accuracy, and make any changes if necessary, then click Finish.
The OVF file is deployed in the selected network.

**Adding a Virtual Hard Disk**

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

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

   **Figure 16: Virtual Appliance Summary Tab**

![Virtual Appliance Summary Tab](image)

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

   **Figure 17: Editing the Virtual Machine Settings**

![Editing the Virtual Machine Settings](image)

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

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

![Virtual Hardware dialog]

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

For the latest information on the recommended disk sizes for a virtual hard disk, refer to the Release Notes in the appropriate version folders at the 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 Policy Manager virtual appliance:

1. To power on the virtual appliance, from the ClearPass Policy Manager virtual appliance, choose **Actions** > **Power On**.
Figure 19: *Powering on the Virtual Appliance*

![Powering on the Virtual Appliance](image)

The virtual appliance is now powered on.

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

**Figure 20: Initial Virtual Machine Console Screen**

![Initial Virtual Machine Console Screen](image)

3. To proceed, enter **y**.
   ClearPass setup and installation begins.
   The following console screen appears:
4. Enter the number for the appropriate appliance type (do not enter the appliance model itself). Options include:
   - 1) CP-SW-EVAL
   - 2) CP-VA-500
   - 3) CP-VA-5K
   - 4) CP-VA-25K

So, for example, to install a CP-VA-500, you would enter the number 2.

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

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

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

ClearPass will reboot at least once.

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

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

The whole installation process process typically takes between 30 and 40 minutes.

7. After the ClearPass virtual appliance launches correctly, the following banner is displayed:
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: eTIPS123
   
   This initiates the ClearPass 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 34.
   
   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.

**Applying and Activating the ClearPass License**

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

To activate and apply the ClearPass license:

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

   \[https://x.x.x.x/tips/\], where \(x.x.x.x\) is the IP address of the management interface defined for the ClearPass server in Table 6.

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

   The Enter License Key screen is displayed.

   **Figure 23: Entering the License Key**

   ![License Key Screen]

3. Do the following:

   a. In the **Select Application** drop-down, make sure the application is set to **Policy Manager**.

   b. Make sure the **I agree to the above terms and conditions** check box is enabled.

   c. In the **Enter license key** text box, enter your ClearPass license key.

   d. Click **Add License**.

   Upon successfully entering the license key, the **Admin Login** screen appears with a message indicating that you have 90 days to activate the product and a link to activate the product.
4. 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 25.

**Figure 25: 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 opens.
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 30.
2. Click Log In.
   The ClearPass Policy Manager Landing Page opens.

   **Figure 27: ClearPass Policy Manager Landing Page**

---

**Signing Up for Live Software Updates**

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

1. Navigate to the Administration > Agents and Software Updates > Software Updates page.
   A message is displayed indicating that the ClearPass virtual appliance is not signed up for live updates and that you must enter your **subscription ID**.

   **Figure 28: Entering the Subscription ID for Live Updates**

2. If the ClearPass Policy Manager server has Internet access, enter your subscription ID, then click **Save**.
   After successfully applying the subscription ID, you will see a message indicating that the subscription ID was updated successfully and ClearPass is processing updates from the ClearPass Webservice.
Note that Posture & Profile Data Updates are downloaded and installed automatically, while Firmware & Patch Updates are merely displayed.

Changing the Administration Password
When the cluster password for this ClearPass server is set upon initial configuration (see Completing the Virtual Appliance Setup on page 30), 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 29: Admin Users Page

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

   Figure 30: Changing the Administration Password

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
- 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
- Applying and Activating the ClearPass License
- Logging in to the ClearPass Virtual Appliance
- Signing Up for Live Software Updates
- 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 into 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 Hyper-V Hypervisors

ClearPass Policy Manager supports the following Hyper-V hypervisors:

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

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

Meeting the Recommended Hyper-V Server Specifications

Carefully review all virtual appliance requirements, including functional IOP ratings, and verify that your system meets these requirements. These recommendations supersede earlier requirements that were published for ClearPass Policy Manager 6.7 installations.
Virtual appliance recommendations are adjusted to align with the requirements for ClearPass hardware appliances. If you don’t have the virtual appliance resources to support a full workload, consider ordering the ClearPass Policy Manager hardware appliance.

**Supplemental Storage/Hard Disk Requirements**

ClearPass Hyper-V ships with a 20 GB hard disk volume. This must be supplemented with additional storage/hard disk by adding a virtual hard disk (see Adding a Hard Disk to a Virtual Machine on page 41 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.

**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 7, and keep it for your records:

**Table 7: ClearPass Server Configuration Information**

<table>
<thead>
<tr>
<th>Required Information</th>
<th>Value for Your Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name (Policy Manager server)</td>
<td></td>
</tr>
<tr>
<td>Management interface IP address</td>
<td></td>
</tr>
<tr>
<td>Management interface subnet mask</td>
<td></td>
</tr>
<tr>
<td>Management interface gateway</td>
<td></td>
</tr>
<tr>
<td>Data interface IP address (optional)</td>
<td></td>
</tr>
<tr>
<td><strong>NOTE:</strong> Make sure that the Data interface IP address is not in the same subnet as the Management interface IP address.</td>
<td></td>
</tr>
<tr>
<td>Data interface subnet mask (optional)</td>
<td></td>
</tr>
<tr>
<td>Data interface gateway (optional)</td>
<td></td>
</tr>
</tbody>
</table>
### 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. From the Aruba Support Center, download the Hyper-V package and copy the files to a folder on your server.
2. Import the virtual machine.
   a. Choose the import type.
   b. If required, specify the virtual switch that the management interface and data interface will be connected to.
3. Add a new virtual hard disk.
   a. Configure the disk format, type, and size based on the requirements for your virtual appliance.
4. Power on and configure the virtual appliance.

Instructions for these procedures are provided in the following sections.

### Importing the Virtual Machine

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

To import the virtual appliance:

1. Download the Hyper-V package from the from the Aruba Support Center > Download Software > ClearPass > Policy Manager > Current Release > Hyper-V folder to a folder accessible by your Hyper-V server.
2. To extract the files, unzip the files to a folder on your server.
3. Open up the Hyper-V Manager Console.
4. From the Hyper-V Manager, select the name of the Hyper-V server, then right-click and select Import Virtual Machine (see Figure 31).
The **Before You Begin** dialog opens.

5. Click **Next**.
   The **Locate Folder** dialog opens.

![Figure 32: Locating the Folder](image)

6. In the **Locate Folder** step, select the folder you unzipped in **Step 1**, then click **Next**.
   The **Select Virtual Machine** dialog opens.

![Figure 33: Selecting the Virtual Machine](image)

7. Make sure the correct virtual appliance is highlighted, then click **Next**.
   The **Choose Import Type** dialog opens.
8. In the **Choose Import Type** step, select **Copy the virtual machine**, then click **Next**.

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

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

**Figure 35: 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.
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.

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

#### Note

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

Figure 40: Configuring the Hard Drive

5. In the Hard Drive dialog:
   a. Controller: Set to IDE Controller 0.
   b. Location: Set to 1 (in use).
5. Below the Virtual hard disk field, click New.
   The New Virtual Hard Disk Wizard opens.
6. From the Before You Begin dialog, click Next.
   The Choose Disk Format dialog opens.
Figure 41: Specifying the Disk Format

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

Figure 42: Specifying the Virtual Hard Disk Type

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

11. Select **Create a new blank virtual hard disk**.
   a. Then enter the size of the virtual hard disk in Gigabytes (GB).

   The recommended virtual hard disk size depends on the number of unique endpoints that will be supported:
   - **EVAL**: 80 GB
   - 500 endpoints: 500 GB
   - 5,000 endpoints: 1000 GB
   - 25,000 endpoints: 1800 GB

   For the latest 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**.
b. When finished, click **Next**.
The **Completing the New Virtual Hard Disk Wizard** screen appears.

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

---

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

---

This completes the procedure to add a virtual hard disk.

### Additional Virtual Hard Disk Considerations

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

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

### Launching the ClearPass Virtual Appliance

To start the Aruba ClearPass Policy Manager virtual appliance:

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

**Figure 45: Starting the Virtual Appliance**

![Virtual Machines](image)

The virtual appliance powers on.

2. To launch the VM console, right-click the name of the virtual machine, then choose **Connect**.
3. To proceed with the installation, enter y.

ClearPass setup and installation begins.

The following console screen appears:
4. Enter the number for the appropriate appliance type (do not enter the appliance model itself). Options include:
   - 1) CP-SW-EVAL
   - 2) CP-VA-500
   - 3) CP-VA-5K
   - 4) CP-VA-25K

So, for example, to install a CP-VA-500, you would enter the number 2.

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

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

6. When you have verified that your system meets the new requirements, press y.
   
   ClearPass will reboot at least once.

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

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

   The whole installation process process typically takes between 30 and 40 minutes.

7. After the ClearPass virtual appliance launches correctly, the following banner is displayed:
8. Proceed to the next section, **Completing the Virtual Appliance Configuration**.

### Completing the Virtual Appliance Configuration

To complete the virtual appliance configuration:

1. **Refer to and note the required ClearPass server configuration information listed in Table 7.**

2. **Log in to the virtual appliance** using the following preconfigured credentials:
   - login: `appadmin`
   - password: `eTIPS123`
   This initiates the Policy Manager Configuration wizard.

3. **Configure the ClearPass virtual appliance.**
   - Follow the prompts, replacing the placeholder entries in the following illustration with the information you entered in Table 7.
   - Enter hostname:
   - Enter Management Port IP Address:
   - Enter Management Port Subnet Mask:
   - Enter Management Port Gateway:
   - Enter Data Port IP Address:
   - Enter Data Port Subnet Mask:
   - Enter Data Port Gateway:
   - Enter Primary DNS:
   - Enter Secondary DNS:

4. **Specify the cluster password.**
   - Setting the cluster password also changes the password for the CLI user `appadmin`, as well as the Administration user `admin`. If you want the `admin` password to be unique, see Changing the Administration Password on page 52.
   
   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 7.
6. **Apply the configuration.**
   a. To apply the configuration, press **Y**.
   b. To restart the configuration procedure, press **N**.
   c. 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.

**Applying and Activating the ClearPass License**

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

To activate and apply the ClearPass license:

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

   `https://x.x.x.x/tips/`
   where `x.x.x.x` is the IP address of the management interface defined for the ClearPass server.

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

   The Enter License Key screen is displayed.

   **Figure 50: Entering the License Key**

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

   Upon successfully entering the license key, the **Admin Login** screen appears with a message indicating that you have 90 days to activate the product and a link to activate the product.
4. To activate ClearPass on this virtual appliance, click **Activate Now**.

When you 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 52.

**Figure 52: 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 53: 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 Configuration on page 48.

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

   **Figure 54: ClearPass Policy Manager Landing Page**

---

**Signing Up for Live Software Updates**

Upon your initial login to ClearPass Policy Manager, we recommend that you register for software updates.

1. Navigate to the **Administration > Agents and Software Updates > Software Updates** page.
   A message is displayed indicating that the ClearPass virtual appliance is not signed up for live updates and that you must enter your **subscription ID**.

   **Figure 55: Entering the Subscription ID for Live Updates**

2. If the ClearPass Policy Manager server has Internet access, enter your **subscription ID**, then click **Save**.
After successfully applying the subscription ID, you will see a message indicating that the subscription ID was updated successfully and ClearPass is processing updates from the ClearPass Webservice. Note that Posture & Profile Data Updates are downloaded and installed automatically, while Firmware & Patch Updates are merely displayed.

### Changing the Administration Password

When the cluster password for this 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.

   ![](figure56.png)

   **Figure 56: Admin Users Page**

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

   ![](figure57.png)

   **Figure 57: Changing the Administration Password**

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

To access the Services Control page:

1. In 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 appears.
3. Select the Services Control tab. The Services Control page opens.

Figure 58: Server Configuration > Services Control Page

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

- If a service is stopped, you can use its Start button to restart it.
- You can also start an individual service from the command line:
  
  service start <service_name>

- You can start all the services from the command line:
  
  service start all
### Summary of the Server Configuration Page

The **Server Configuration** page provides many options. Table 8 describes each of the top-level server configuration options that are available. For details, refer to the "Server Configuration" chapter in the ClearPass Policy Manager User Guide.

**Table 8: Description of the Server Configuration Page**

<table>
<thead>
<tr>
<th>Tab</th>
<th>Description</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
<td>Displays server identity and connection parameters.</td>
<td></td>
</tr>
<tr>
<td><strong>Services Control</strong></td>
<td>You can view the status of a ClearPass Policy Manager service (that is, see whether a service is running or not), and stop or start services.</td>
<td></td>
</tr>
<tr>
<td><strong>Service Parameters</strong></td>
<td>This option allows you to change the system parameters for all services.</td>
<td>The options on this page vary based on the service selected.</td>
</tr>
<tr>
<td><strong>System Monitoring</strong></td>
<td>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.</td>
<td>This ensures that external Management Information Base (MIB) browsers can browse the system-level MIB objects exposed by the ClearPass Policy Manager appliance. The options on this page vary based on the SNMP version that you select.</td>
</tr>
<tr>
<td><strong>Network</strong></td>
<td>Use the Network page to: &lt;ul&gt;&lt;li&gt;Create generic routing encapsulation (GRE) tunnels and VLANs related to guest users.&lt;/li&gt;&lt;li&gt;Control which applications can have access to the node.&lt;/li&gt;&lt;/ul&gt;</td>
<td>&lt;ul&gt;&lt;li&gt;A GRE tunnel creates a virtual point-to-point link between controllers over a standard IP network or the Internet.&lt;/li&gt;&lt;li&gt;To create VLANs, your network infrastructure must support tagged 802.1Q packets on the physical interface selected.&lt;/li&gt;&lt;li&gt;VLAN ID 1 is often reserved for use by certain network management components&lt;/li&gt;&lt;/ul&gt;<strong>NOTE:</strong> Avoid using VLAN ID 1 unless you know it will not conflict with a VLAN already defined in your network.</td>
</tr>
<tr>
<td><strong>FIPS</strong></td>
<td>Enables ClearPass to operate in Federal Information Processing Standard mode.</td>
<td>For most users, this tab should be ignored. <strong>NOTE:</strong> Enabling FIPS mode resets the database.</td>
</tr>
</tbody>
</table>

### Subset of CLI for ClearPass Maintenance Tasks

The Command Line Interface (CLI) provides a way to manage and configure ClearPass 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 console to run the virtual appliance.

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

******************************************************************************
CLI Task Examples

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

[appadmin]# show ip

Reconfigure DNS or Add a New DNS

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

Reconfigure or Add Management and Data Ports

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

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| ip <mgmt|data> <ip address> | - Network interface type: mgmt or data
|                     | - Server IP address                              |
| netmask <netmask address> | Netmask address                                        |
| gateway <gateway address> | Gateway address                                        |

Configure the Date

Configuring the time and time zone is optional.

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

Configure the Host Name for the Node

[appadmin]# configure hostname <hostname>

Join the 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 (for more information, see Joining an Active Directory Domain on page 1).

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

<table>
<thead>
<tr>
<th>Flag/Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;domain-controller.domain-name&gt;</td>
<td>Required. This is the name of the host to be joined to the domain. <strong>NOTE:</strong> Use the Fully Qualified Domain Name.</td>
</tr>
<tr>
<td>[domain NetBIOS name]</td>
<td>Optional.</td>
</tr>
</tbody>
</table>