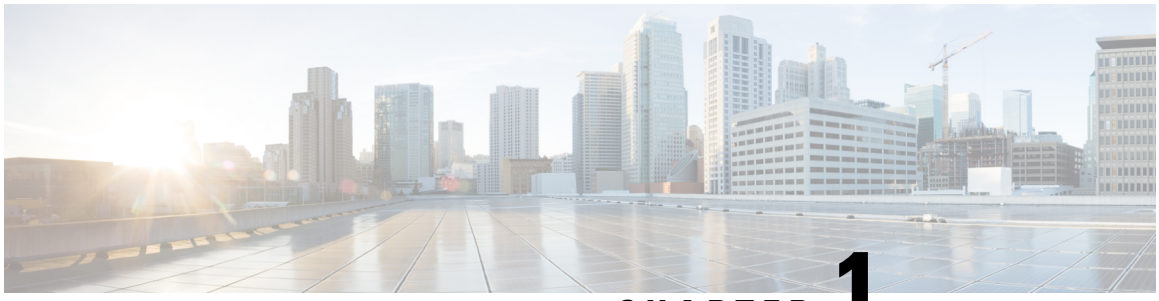
Installation Guide for Cisco Evolved Programmable Network Manager 3.0

First Published: 2018-12-03

Last Modified: 2019-02-28

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco EPN Manager 3.0 Installation

This chapter provides the information required for planning your installation of Cisco EPN Manager 3.0 and ensuring that you meet all the prerequisites required for the installation. It also provides procedures for installing Cisco EPN Manager 3.0 in a standard, non-high availability environment. For high availability, see Cisco EPN Manager 3.0 High Availability Installation, on page 25.

Installation Overview

Cisco EPN Manager 3.0 can be installed as a fresh installation either on a virtual machine or a bare metal server. If you are already using a previous version of Cisco EPN Manager, you can upgrade to Cisco EPN Manager 3.0 and thereby retain your data. See Upgrade to Cisco EPN Manager 3.0, on page 33.

The following topics provide an overview of the Cisco EPN Manager 3.0 installation and upgrade options and provide additional useful installation-related information.

Note After installing any release or maintenance pack, it is recommended to check the Software Download site on Cisco.com for point patches and to install the latest available point patch for that release or maintenance pack. Information about the point patch and installation instructions can be found in the readme file supplied with the patch file on the Software Download site on Cisco.com.

Installation Options

You can install Cisco EPN Manager 3.0 either on a virtual machine (VM) or a bare metal server:

- OVA/VM installation—For a VM installation, install the Open Virtual Appliance (OVA) file on a dedicated server that complies with the requirements listed in OVA/VM Requirements. We recommend that you run only one Cisco EPN Manager VM instance per server hardware.
- ISO/bare metal installation—For a bare metal server installation, install the ISO image, which acts as a virtual boot that supports the Cisco Unified Computing System (UCS) server installation. The requirements are listed in Bare Metal Requirements. You can also use the ISO image to install Cisco EPN Manager on a VM. A built-in terminal or console server application called Cisco Integrated Management Controller (Cisco IMC) is used to install Cisco EPN Manager on the bare metal Cisco UCS server hardware.

Note ISO/Bare metal installation is not supported on non-Cisco hardware. To install Cisco EPN Manager on non-Cisco hardware, use VMware and install the OVA file. Using VMware will minimize hardware non-compliance issues, however, you must make sure that your hardware has the resources required to allow provisioning of the VM.

Both OVA and ISO installations include the following:

- RHEL 7.4 operating system
- Oracle Database 12c Enterprise Edition Release 12.1.0.2 (64-bit production)
- EPN Manager

Note Cisco EPN Manager does not support independent user-installed Linux/Oracle patches. Any necessary patches are included in Cisco EPN Manager releases or point patches.

Note Cisco EPN Manager does not support 4K sector disk.

Firmware Upgrade

Cisco EPN manager does not support Firmware or any product upgrades. If you need any support on the upgrades, please contact your Cisco Advanced Services representative.

Dual NIC Installation

These topics describe how to perform Dual NIC installation:

• Remove IP Configuration, on page 3

Prerequisites

In an HA environment:

- Remove High Availability
- Add the configuration needed for the second NIC
- Perform High Availability registration between Primary and Secondary Servers

Configure the Second NIC on Primary

Enter these commands in the admin CLI.

```
storm-ha-194/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
storm-ha-194/admin(config)# interface GigabitEthernet 1
storm-ha-194/admin(config-GigabitEthernet)# ip address 172.23.222.32 255.255.255.0
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
Are you sure you want to proceed? [y/n] y
storm-ha-194/admin(config-GigabitEthernet)# end
```

Add Static Route for Device Subnets in Primary

```
storm-ha-194/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
storm-ha-194/admin(config)# ip route 172.0.0.0 255.0.0.0 gateway 172.23.222.32
storm-ha-194/admin(config)# end
storm-ha-194/admin# write memory
```

Update /etc/hosts in Multi NIC Server

By default, when we add eth1, it gets added to /etc/hosts with the hostname as eth0. We have to update the hostname of eth1 with its value.

Operation of a Multi-NIC Server

Static routes are not migrated as part of Backup restore process. We need to configure it manually after a restore. However, this setting can be retained in the upgraded [Backup Restore Upgrade] server.

In a HA environment:

- Failure of the first interfaces (used for heartbeat (the first interface)) will trigger a HA failover.
- Failure of the 2nd interface (SBI interface) will also trigger a failover.

Remove IP Configuration

```
storm-ha-194/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
storm-ha-194/admin(config)# interface gigabitEthernet 1
storm-ha-194/admin(config-GigabitEthernet)# no ip 172.23.222.32 255.255.255.0
```

Upgrade Options

You can upgrade to Cisco EPN Manager 3.0 by following the valid upgrade path relevant for your existing deployment. See Valid Upgrade Paths, on page 33.

The following methods are available for upgrading to Cisco EPN Manager 3.0:

- In-Place Upgrade—This option is usually chosen when you are not using new hardware; in other words, you are performing the upgrade on the machine that is running the earlier version of Cisco EPN Manager. There is some downtime with this type of upgrade but after the upgrade, you do not have to restore your data from a backup. For more information, see In-Place Upgrade.
- Backup-Restore Upgrade—This upgrade option generally requires new hardware (although it is possible to use existing hardware). There is less downtime when performing this type of upgrade as the current version of Cisco EPN Manager remains operational while you install the new version on the new hardware. However, after the installation, you must restore your data from a backup. After starting the restore process, there will be a period during which some data will not be available on the new server until all the data has been copied over. For more information, see Backup-Restore Upgrade.

Note Cisco EPN Manager does not support automatic rollback to the previous version after an upgrade but you can manually revert to the previous version. See Revert to the Previous Version of Cisco EPN Manager for more information.

Users Created During Installation

The following types of users are created during the installation process:

- **Cisco EPN Manager CLI admin user**—Used for advanced administrative operations such as stopping and restarting the application and creating remote backup repositories. Provides access to the CEPNM Admin CLI, a Cisco proprietary shell which provides secure and restricted access to the system (as compared with the Linux shell).

  The password for the CLI admin user is user-defined during installation but can be changed at a later stage by entering the following command:

  ```
  admin(config)# username admin <Password>
  ```

- **Linux CLI admin user**—Used for Linux-level administration purposes. Provides access to the Linux CLI, a Linux shell which provides all Linux commands. The Linux shell should only be used by Cisco technical support representatives. Regular system administrators should not use the Linux shell. The Linux shell can only be reached through the Cisco EPN Manager admin shell and CLI. The Linux CLI admin user can get Linux root-level privileges, primarily for debugging product-related operational issues.
- **Cisco EPN Manager web GUI root user**—Required for first-time login to the web GUI, and for creating other user accounts. The root user password is user-defined at the time of installation.
- **ftp-user**—Used for internal operations like image distribution to device or other operations that access external servers using FTP. The password is randomly generated and is changed periodically. Users with Admin privileges can change the ftp user password but this user-defined password will expire after a few months. Use this command to change the ftp user password:

  ```
  admin# ncs password ftpuser username password password
  ```

- **scpuser**—Used for internal operations like image distribution to device or other operations that access external servers using SCP. The password is randomly generated and is changed periodically.
- **prime**—The system-generated account under which all the application processes run. No changes can be made.
- **oracle**—The system-generated account used by the Oracle process. No changes can be made.

Note The first four user accounts are associated with actual network users. Cisco EPN Manager uses the **scpuser**, **prime**, and **oracle** user accounts to perform internal operations and they cannot be changed in any way.

For more information about user types and managing users, see the Cisco Evolved Programmable Network Manager User and Administrator Guide.

System Requirements

The following sections list the requirements that must be met before installing Cisco EPN Manager 3.0:

- Hardware and Software Requirements
- Web Client Requirements
- Scale Requirements (Professional)
- Ports Used by Cisco EPN Manager

Hardware and Software Requirements

- OVA/VM Requirements
- Bare Metal Requirements

OVA/VM Requirements

The following table summarizes the OVA/VM system requirements for the Standard and Professional system size options:

- **Standard:** To be used in a pre-production environment for lab tests, demos, and so on. Not recommended for use in a production environment.
- **Professional:** Recommended for production environments that meet the minimum requirements.

It is not recommended to use the Express and Express Plus system size options. Furthermore, the Compliance functionality is not supported on Express and Express Plus system size options.

Note External storage is supported for OVA/VM installations.

Server Type	Item	Standard	Professional
Virtual Machine	VMWare ESXi version **Note** Installations using an OVA image are supported on VMWare ESXi or ESX, on your own hardware. In all cases your server must meet or exceed the requirements listed in this table.	6.0.x, 6.5	6.0.x, 6.5
	Appliance image format	OVA	OVA
Hardware	Virtual CPU (vCPU)	16	16
	Memory (DRAM)	48 GB	64 GB
	Disk Capacity	900 GB	1200 GB
	Disk I/O speed	350 MBps	Minumum: 350 MBps Full scale: 450 MBps

Bare Metal Requirements

For bare metal installations, Cisco EPN Manager can only be installed on the Cisco UCS server (UCS C220 M4 or M5) as a rack-mounted server with the requirements listed in the following sections.

External storage is not supported for bare metal installations.

Note As opposed to OVA/VM installations, bare metal installations will use the full server resources.

Bare Metal Requirements for Standard Deployments (No High Availability)

These are the minimum requirements for a standard deployment (no high availability).

Item		Requirement
Bare-Metal	Appliance image format	ISO
	Equivalent 1.x Option	Physical Server

Hardware	Cisco UCS server type	Cisco UCS C220 M4, M4S, M5, M5SX and M5L
	CPU (cores/threads)	1 x CPU (10 C/20 T)
	Memory	64 GB
	Disk capacity	4x900 GB
	Disk I/O speed	450 MBps
	RAID Level	RAID 10

Bare Metal Requirements for Remote High Availability Deployments

These requirements are for a remote high availability deployment. A remote deployment is one in which both servers are located on different subnets connected by a WAN. This is typical for deployments when the servers are geographically dispersed. For more information on high availability deployments, see Cisco EPN Manager 3.0 High Availability Installation, on page 25.

Hardware	Requirement
Cisco UCS server type	Cisco UCS C220 M4, M4S, M5, M5SX and M5L
CPU speed	Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz or above
Cores/threads	10 C/20 T
Storage adapter	Cisco 12G SAS Modular Raid Controller
Hard Disk	Product ID: Cisco 12G SAS Modular Raid Controller
Interface	SATA (Serial Advanced Technology Attachment)
Hardware Sector Size	512 Native **Note** 4K sector disk is not yet supported
Memory	64 GB
RAID level	RAID 10
Number of NICs	1
Disk capacity	4x900 GB
Virtual hard disk size in RAID controller	1 TB (minimum requirement)
Hard disk controller location	Slot 1
Hard disk I/O speed	450 MBps
Hard disk RPM	Minimum 15k RPM SAS (flash recommended)

Hardware	Requirement
Network bandwidth	Ideal: 977 Mbps Minimum: 255 Mbps or more
Latency	Less than 100 msecs

Web Client Requirements

The following are the client and browser requirements for the Cisco EPN Manager Web GUI:

- Hardware—Mac or Windows laptop or desktop compatible with one of the tested and supported browsers listed below.
- Browsers:
  - Google Chrome versions 44 to 70
  - Mozilla Firefox ESR 38
  - Mozilla Firefox versions 39 to 63
  - Microsoft Internet Explorer (IE) 11.0

Note Internet Explorer users have reported slower performance compared to other browsers, meaning that some GUI pages take longer to load in IE.

- Recommended display resolution—1600x900 pixels or higher (minimum: 1366x768)

Note A maximum of three Cisco EPN Manager tabs can be open simultaneously in a single browser session.

Scale Requirements (Professional)

The following table summarizes the maximum level of support for a professional system size deployment in both OVA/VM and ISO/bare metal installations (based on test results from this example set of devices).

These scale numbers are for a Cisco EPN Manager Professional deployment that uses the default system settings. The numbers represent an example combination of different devices for each device type. Keep in mind that scale considerations depend on a number of factors including interface count, polling frequency, and so on.

Note You are highly recommended to contact your Cisco representative for assistance in determining the number of instances of Cisco EPN Manager you require before purchasing licenses and starting the implementation.

Item	Description	Maximum
Packet devices	Cisco Aggregation Services Routers (ASR) 9000 Series	100
	Cisco Aggregation Services Routers (ASR) 920 Series	1,100
	Cisco Aggregation Services Routers (ASR) 903 Series	500
	Cisco Aggregation Services Routers (ASR) 901 Series	1,100
	Cisco ME 3800X Series Carrier Ethernet Switch Routers	1,100
	Cisco ME 3600X Series Carrier Ethernet Switch Routers	1,100
	Maximum total packet devices	5,000
Optical devices	Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 Series devices	3,000
	Cisco Network Convergence System (NCS) 4000 Series	1,000
	Maximum total optical devices	4,000
Optical and packet devices (hybrid)	Maximum total optical and packet devices (hybrid)	5000
Cable devices	Maximum total cBR-8 devices	200
	Maximum total Remote Physical Devices (RPDs) **Note** For information about optimizing Cisco EPN Manager performance, please contact your Cisco representative.	5,000
Monitoring	Sustained rate of events (events/sec)	100
	Maximum interfaces in the system	350000
	Maximum interfaces per device **Note** Limited to 10 devices with the maximum number of interfaces per system.	4000
System users	Concurrent web GUI users	50
	Concurrent API users	5

Ports Used by Cisco EPN Manager

Note The installation process uses the server's eth0 and eth1 Ethernet ports. If you use a different port, the system might not work properly.

The following table lists the ports that Cisco EPN Manager uses to listen for connection requests from devices. For security hardening, this table also specifies whether it is safe to disable the port without any adverse effects to the product.

As a general policy, any ports that are not needed and are not secure should be disabled. You need to first know which ports are enabled, and then decide which of these ports can be safely disabled without disrupting the normal functioning of Cisco EPN Manager. You can do this by listing the ports that are open and comparing it with a list of ports that are safe to disable. The built-in firewall in Cisco EPN Manager does not expose some of the listening ports. To view a list of the ports used in your deployment, log in as a Cisco EPN Manager CLI admin user and run the **show security-status** command. To view a list of all open listening ports, including those that are blocked by the built-in firewall, log in as the Linux CLI admin user and run the **netstat -aln** command.

In addition to the built-in firewall, you can also deploy additional network firewalls to block other unused ports and their traffic.

Table 1: Listening Ports That Are Open Through Built-in Firewall

Port	Protocol	Usage	Safe to Disable?	Notes
21	TCP	To transfer files to and from devices using FTP.	Yes	Disable FTP from the web GUI under **Administration > Settings > System Settings**, then choose **General > Server**. After disabling FTP, as the CLI admin user, stop and restart the server.
22	TCP	To initiate SSH connections with the Cisco EPN Manager server, and to copy files to the Cisco EPN Manager server using SCP or SFTP.	Depends	This might be still needed by older managed devices that only support TFTP and not SFTP or SCP.
69	UDP	To distribute images to devices using TFTP.	Depends	Only if alternative protocols like SCP or SFTP or HTTPS are used for image distribution, and if supported by the managed devices.
162	UDP	To receive SNMP traps from network devices.	No	—
443	TCP	For browser access to the Cisco EPN Manager server via HTTPS.	No	—
514	UDP	To receive syslog messages from network devices.	No	—
1522	TCP	For High Availability (HA) communication between active and standby Cisco EPN Manager servers. Used to allow Oracle JDBC traffic for Oracle database synchronization.	Yes	If at least one Cisco EPN Manager server is not configured for HA, this port is automatically disabled.

Port	Protocol	Usage	Safe to Disable?	Notes
2021	TCP	To distribute images to devices using FTP.	No	—
8082	TCP	For the HA Health Monitor web interface (via HTTP). Used by primary and secondary servers to monitor their health status via HTTP.	No (If HA configured)	—
8087	TCP	To update software on the HA secondary backup server (uses HTTPS as transport).	No	—
9991	UDP	To receive Netflow data packets.	Yes	Cisco EPN Manager does not support Netflow. You should disable this traffic in the network firewall.
9992	TCP	To manage M-Lync using HTTP or HTTPS.	Yes	Cisco EPN Manager does not support M-Lync. You should disable this traffic in the network firewall.
11011 to 11014	TCP	For PnP operations for proprietary Cisco Network Service (CNS) protocol traffic.	Yes	Cisco EPN Manager does not support PnP. You should disable this traffic in the network firewall by entering the following commands in this sequence (as the Cisco EPN Manager CLI admin user): **ncs pnp-gateway disable** **ncs stop** **ncs start**
61617	TCP	For MTOSI NBI notification over Java Message Service (JMS) connections. Also used for PnP operations.	Yes	Cisco EPN Manager does not support MTOSI over JMS or PnP. You should disable this traffic in the network firewall.

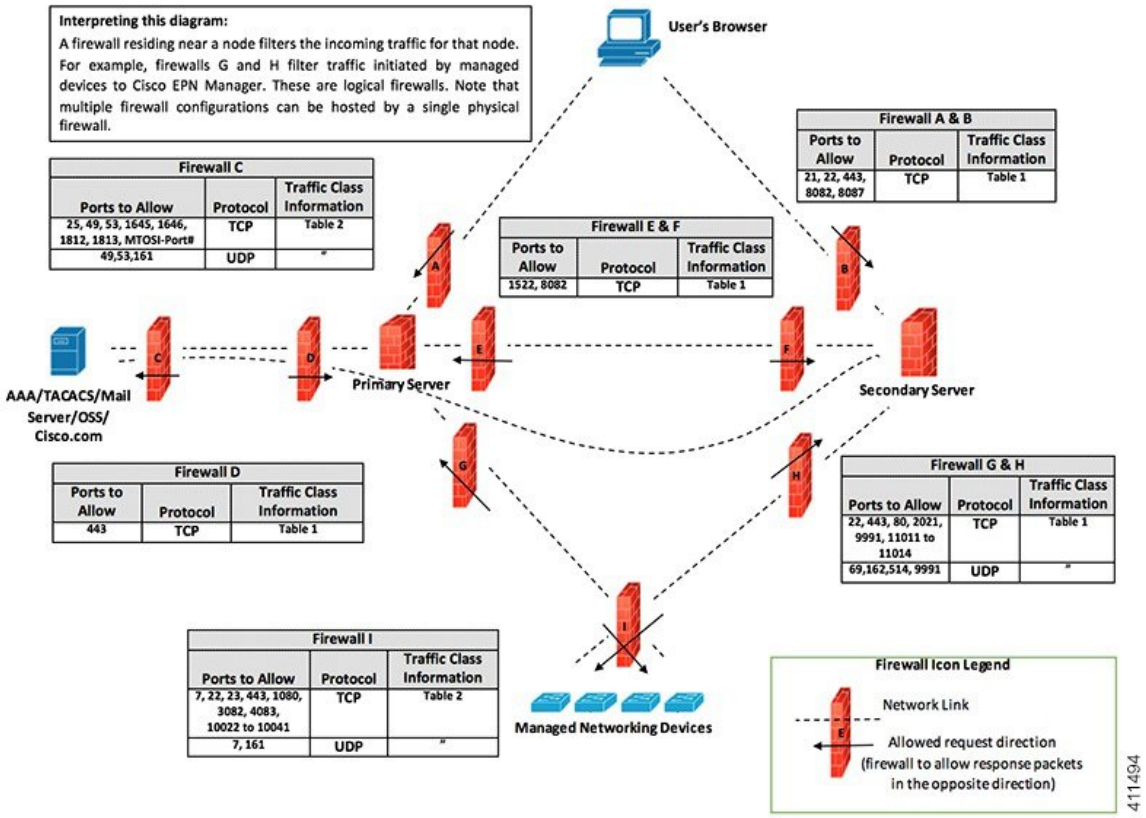
The following table lists the destination ports on external devices that may be protected by a firewall. These ports are used by Cisco EPN Manager to connect to network devices. You must open the required ports to allow Cisco EPN Manager to connect to these devices.

Table 2: Destination Ports Used by Cisco EPN Manager

Port	Protocol	Used to:
7	TCP/UDP	Discover endpoints using ICMP.
22	TCP	Initiate SSH connections with managed devices.

Port	Protocol	Used to:
23	TCP	Communicate with managed devices using Telnet.
25	TCP	Send email using an SMTP server.
49	TCP/UDP	Authenticate Cisco EPN Manager users using TACACS.
53	TCP/UDP	Connect to DNS service.
161	UDP	Poll using SNMP.
443	TCP	Upload or download images and perform configuration backup-restore for Cisco NCS 2000 devices using HTTPS.
1522	TCP	Communicate between primary and secondary HA servers (allows Oracle JDBC traffic for Oracle database synchronization between primary and secondary servers).
1080	TCP	Communicate with Cisco Optical Networking System (ONS) and Cisco NCS 2000 series devices using Socket Secure (SOCKS) protocol.
1645, 1646, and 1812, 1813	UDP	Authenticate Cisco EPN Manager users using RADIUS.
3082	TCP	Communicate with Cisco ONS and Cisco NCS 2000 devices using TL1 protocol.
4083	TCP	Communicate with Cisco ONS and Cisco NCS 2000 series devices using secure TL1 protocol.
8082	TCP	Communicate between primary and secondary HA servers to monitor each other's health using HTTPS.
10022 to 10041	TCP	Passive FTP file transfers (for example, device configurations and report retrievals).
MTOSI/RESTCONF TCP port number	TCP	Listen at NBI client connected to the Cisco EPN Manager server (after this port is configured by NBI client system, a registration notification message containing the port number is sent to Cisco EPN Manager server); refer to the MTOSI or RESTCONF API guide for more information.

The following figure illustrates the ports information listed in the previous tables. Use this illustration to decide on the appropriate firewall configuration (allowing correct incoming traffic) for your network infrastructure. To identify the class of traffic, refer to the Usage column in Table *Listening Ports That Are Open Through Built-in Firewall* . We recommend that you disable the ports that are used by services that are not supported in Cisco EPN Manager.



Installation Prerequisites

Licensing

Cisco EPN Manager includes a 90-day trial license that is automatically activated for first-time installations. To use the application beyond the trial period, you must obtain and install the necessary Cisco EPN Manager licenses for both production and non-production environments, as follows:

For a production environment:

- Base license (required)
- Standby license (optional)—Obtain this license if you will have a high availability deployment with two Cisco EPN Manager servers configured in a redundancy configuration.
- NBI license (optional)—Obtain this license if you will be using MTOSI or RESTCONF northbound interface features
- Right-to-Manage licenses for the types and corresponding numbers of devices to be managed by Cisco EPN Manager

For a non-production environment (e.g., lab validation or development environment), please obtain and install a Cisco EPN Manager lab license for each Cisco EPN Manager lab installation. The lab license covers all Cisco EPN Manager options, including redundancy (HA), and unlimited right-to-manage scope.

Do not make copies of licenses.

To purchase Cisco EPN Manager licenses, please contact your local sales representative.

For more information on the types of licenses available for Cisco EPN Manager, see the information on viewing and managing licenses in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Prerequisites for OVA/VM Installations

Before installing Cisco EPN Manager on a virtual machine, ensure that:

- Your deployment meets the general hardware and software requirements listed in System Requirements, and specifically in OVA/VM Requirements.
- Hardware resources are reserved for the Cisco EPN Manager server to ensure optimal performance. CPU minimum clock is 2.2 Ghz per CPU.
- VMware ESX/ESXi is installed and configured on the machine you plan to use as the Cisco EPN Manager server. See the VMware documentation for information on setting up and configuring a VMware host.
- The installed VMware ESX/ESXi host is reachable.
- The VMware vSphere client is installed on a Windows host (or laptop). See the VMware documentation for information on how to install the VMware vSphere client. After the virtual host is available on the network, you can browse to its IP address to display a web-based interface from which you can install the VMware vSphere client. The VMware vSphere client is Windows-based, so you must download and install the client using a Windows PC.
- The Cisco EPN Manager OVA is saved to the same machine where your VMware vSphere client is installed.
- The downloaded OVA package has been verified as described in Verify the ISO Image or OVA Package.

Prerequisites for ISO/Bare Metal Installations

Before installing Cisco EPN Manager using an ISO image, ensure that:

- Your deployment meets the general hardware and software requirements listed in System Requirements, and specifically in Bare Metal Requirements.
- The following software is installed:
  - Java with JRE Version 1.6.0.14 or higher
  - Flash Driver v9.0.246 or higher
- The downloaded ISO image has been verified as described in Verify the ISO Image or OVA Package.
- A reliable link is available for accessing the installation file. VPN links are not recommended.

Verify the ISO Image or OVA Package

Before installing Cisco EPN Manager, you need to verify the ISO image or OVA package. You do not need to verify the individual UBF files that are bundled inside the ISO image or OVA package.

Step 1 If you do not have **openssl** installed, download and install it (see http://www.openssl.org).

Step 2 Download the following files from the Software Download site on Cisco.com, and place them in a temporary directory.

- The Cisco EPNM 3.0 product OVA package or ISO image to be verified (*.iso or *.ova)
- The Cisco EPNM 3.0 OVA or ISO signature file (*.signature)
- The Cisco EPNM 3.0 certificate file (*.pem)

(The same certificate file (*.pem) is used to validate OVA and ISO files.)

Step 3 Move the ISO or OVA files, the certificate file, and the signature file to an alternate RHEL machine with openssl capability using a transfer method such as scp.

Step 4 Run the following command:

```
openssl dgst -sha512 -verify cert-file -signature sig-file product-file
```

Where:

- *cert-file* is the certificate file (*.pem)
- *sig-file* is the signature file (*signature)
- *product-file* is the file to be verified

Step 5 If the result is **Verified OK**:

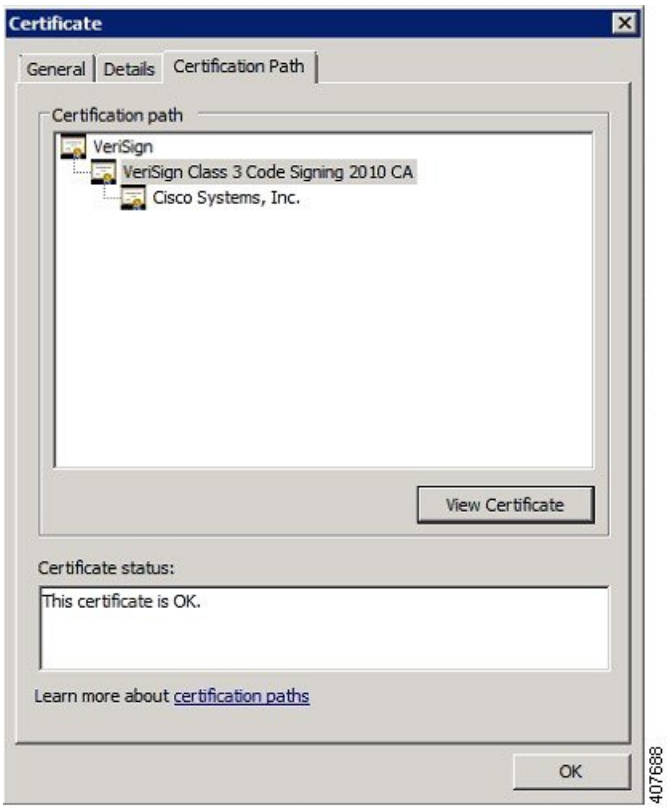
- For an OVA package, proceed to *Step 6*.
- For an ISO file, go to Install Cisco EPN Manager 3.0 (No HA).

Step 6 (OVA packages only) Verify the publisher and certificate chain using the VMware vSphere client.

1. Verify that Cisco Systems is the publisher:
   1. In the VMware vSphere client, choose **File > Deploy OVF Template**.
   2. Browse to the OVA installation file (*.ova) and select it, then click **Next**.
   3. Check whether the Publisher field in the OVF Template Details window displays **Cisco Systems, Inc** with a green check mark next to it. Do not proceed if the Publisher field displays **No certificate present**. This indicates that the image is not signed or the file is not from Cisco Systems or the file has been tampered with. Contact your Cisco representative.

      Note Do not validate the image using the information in the Vendor field. This field does not authenticate Cisco Systems as the publisher.

2. Check the certificate chain:
   1. In the OVF Template Details window, click the **Cisco Systems, Inc.** hyperlink in the Publisher field.
   2. In the Certificate window, click the **Certification Path** tab.
   3. In the Certification Path tab (which lists the certificate chain), ensure that the Certification Path area displays **Cisco Systems, Inc.** and the Certificate Status displays **This certificate is OK**, as shown in the following figure.



Install Cisco EPN Manager 3.0 (No HA)

Install Cisco EPN Manager Using an OVA/VM

1. Make sure your deployment meets the requirements in System Requirements.
2. Make sure your deployment meets the prerequisites in Prerequisites for OVA/VM Installations. This includes verifying the OVA package.
3. Deploy the OVA from the VMware vSphere Client.
4. Set the System Time of the Deployed OVA, on page 17
5. Install Cisco EPN Manager on the Server.
6. Uninstall Cisco EPN Manager.

Deploy the OVA from the VMware vSphere Client

Step 1 Launch the VMware vSphere client.

Step 2 Choose **File > Deploy OVF Template**.

Step 3 In the Deploy OVF Template window, click **Browse**.

Step 4 Navigate to the OVA file, select it, then click **Next**.

Step 5 Accept the End User License Agreement, and in the OVF Template Details window, verify the OVA file details including the product name, version, and size, then click **Accept**.

Step 6 In the Name and Location window:

1. Specify a name and location for the template that you are deploying. The name must be unique within the inventory folder, and can contain up to 80 characters.
2. Select the configuration type as Standard or Professional based on your network size (see System Requirements).
3. Click **Next**.

Step 7 Select the cluster or host on which to install the OVA, then click **Next**.

Step 8 Select the destination storage for the OVA to be deployed, then click **Next**.

Step 9 Select the disk format as **Thick Provision Lazy Zeroed** or **Thick Provision Eager Zeroed**, then click **Next**.

Step 10 Select the network mapping based on the configured IP address, then click **Next**.

Step 11 In the Ready to Complete window:

1. Verify your selections.
2. (Optional) If you want the virtual machine to automatically start after the OVA deployment has finished, check the **Power on after deployment** check box.
3. Click **Finish**.

This process might take a few minutes to complete. Check the progress bar in the Deploying Virtual Application window to monitor the task status. When the deployment task has successfully completed, a confirmation window appears.

Step 12 Click **Close**. The virtual appliance that you deployed is listed under the host, in the left pane of the VMware vSphere client.

What to do next

Proceed to Set the System Time of the Deployed OVA, on page 17.

Set the System Time of the Deployed OVA

Step 1 In the VMware vSphere client, select the VM in the left pane.

Step 2 Access the Boot Settings options (**Edit Settings>VM Options> Boot Settings**.

Step 3 Select the check box in the **Force BIOS Setup** area so that the BIOS setup screen will appear the next time the VM boots.

Step 4 Click **Save**.

Step 5 Boot the VM.

Step 6 In the BIOS setup screen, set the system time and date to the current UTC time.

Step 7 Press **F10** to save your changes and exit the screen.

What to do next

Proceed to Install Cisco EPN Manager on the Server.

Install Cisco EPN Manager on the Server

Step 1 In the VMware vSphere client, click the **Console** tab, and at the localhost login prompt, enter **setup**.

Step 2 Enter the following parameters as you are prompted for them:

Parameter	Description
Hostname	Host name of the virtual machine.
IP Address	IP address of the virtual machine.
IP default netmask	Default subnet mask for the virtual machine IP address.
IP default gateway	IP address of the default gateway.
Default DNS domain	Default DNS domain name.
Primary nameserver	IP address of the primary DNS server. The console will prompt you to add a secondary nameserver. Enter: • **Y** to enter a secondary nameserver. • **N** to proceed to the next step of the installation.
Secondary nameserver	IP address of the secondary DNS server you want to use if the primary server cannot be reached.
Primary NTP server	IP address or host name of the primary Network Time Protocol server you want to use (the default is **time.nist.gov**). The console will prompt you to add a secondary NTP server. Enter: • **Y** to enter a secondary NTP server. • **N** to proceed to the next step of the installation.
Secondary NTP servers	IP address of the secondary NTP server you want to use if the primary NTP server cannot be reached.
System Time Zone	The time zone you want to use.
Clock time	The clock time (based on the selected System Time Zone). This is the time that will be shown in the machine. Check that the time is correct based on your time zone and change it if necessary. See Time Zones Supported by Cisco Evolved Programmable Network Manager, on page 56. The console will prompt you to change the system clock time. Enter: • **Y** to change the clock time. • **N** to proceed to the next step of the installation.

Parameter	Description
Username	The name of the first administrative user (**admin** by default). This is the Cisco EPN Manager **CLI admin user** that logs into the Cisco EPN Manager server using SSH.
Password	The password for the first administrative user. The password must be at least 8 characters long, and must contain at least one number and one upper-case letter.

When you have entered the necessary values, the installer application tests the network configuration parameters you entered. If the tests are successful, it begins installing Cisco EPN Manager.

Step 3 When the application installation is complete, you will be prompted to choose whether you want the newly-installed server to act as a secondary server in an HA implementation.

- Enter **yes** if you are using HA and you want this server to be the secondary server. Do not continue with the next step; go to Install Cisco EPN Manager 3.0 in a High Availability Deployment, on page 30.
- Enter **no** if:
  - You are not using HA.
  - You are using HA but you want this server to be the primary server.

Step 4 Enter a password for the Cisco EPN Manager **web GUI root user** (you will have to enter it twice). You will use this password to log into the web GUI for the first time and create other user accounts. (This account should be disabled after you create a new user account with the same level of privileges.)

Step 5 Review your settings and:

- If the settings are correct, select **Y** to apply them.
- If any settings are incorrect, select **N**, edit them, and then apply them.

Step 6 (ISO/Bare Metal deployments) When the installation is complete:

1. After the server reboots and you are presented with a login prompt, log in using the Cisco EPN Manager CLI admin username and password you configured.
2. Synchronize the hardware and NTP clocks as described in Synchronize the Hardware and NTP Clock.

Step 7 (OVA/VM deployments) When the installation is complete and the virtual machine has rebooted:

1. Log into the virtual machine using the Cisco EPN Manager CLI admin username and password you configured in *Step 3*.
2. Stop and restart the Cisco EPN Manager server using the following commands:

```
ncs stop
ncs start
```

Install Cisco EPN Manager Using an ISO/Bare Metal Image

1. Make sure your deployment meets the requirements in System Requirements.
2. Make sure your deployment meets the prerequisites in Prerequisites for ISO/Bare Metal Installations. This includes verifying the ISO/bare metal image.

3. Configure the Cisco IMC Server.
4. Configure the Bare Metal Cisco UCS Server.
5. Install Cisco EPN Manager from an ISO Image.
6. Uninstall Cisco EPN Manager.

Note The installation procedure provided in these sections is specific to the UCS server type and hardware requirements described in Bare Metal Requirements.

Configure the Cisco IMC Server

Cisco Integrated Management Controller (Cisco IMC) is the server management application that you can use to remotely access, configure, administer, and monitor the Cisco EPN Manager server.

Step 1 To access the console, attach a keyboard and monitor to the USB ports on the rear panel of the appliance or by using a KVM cable and connector.

Step 2 Power on the Cisco UCS server.

Step 3 Press **F8** to enter the Cisco IMC configuration utility. You will need to press the function keys (F8, F6 and F2) more than once until the system responds. If you do not press **F8** quickly enough and enter the EFI shell, press **Ctrl-Alt-Del** to reboot the system and press **F8** again.

Step 4 In the Cisco IMC Configuration Utility window, from the IPV4 (Basic) area, enter the following:

- DHCP Enabled—Select this option to enable DHCP for dynamic network settings. Before you enable DHCP, your DHCP server must be preconfigured with the range of MAC addresses for this server.
- Cisco IMC IP—Enter the IP address of Cisco IMC.
- Subnetmask—Enter the subnet mask to append to the Cisco IMC IP address. It must be in the same subnet as the host router.
- Gateway—Enter the IP address of the default gateway router.

Step 5 Press **F5** to refresh the page and display the new settings.

Step 6 (Optional) In the VLAN (Advanced) area, configure VLAN settings.

Step 7 Enter the Cisco IMC password. If you leave the Username and Password fields blank, the system uses the following default login credentials:

- Username: **admin**
- Password: **password**

Step 8 When a prompt is returned, press **F10** to save the configuration.

Step 9 Update the following fields as specified:

- NIC mode—Select **Dedicated**.
- IP (Basic)—Select **IPV4**.
- DHCP—Disable DHCP if enabled.
- CIMC IP—Enter the IP address of the Cisco IMC.

- Prefix/Subnet—Enter the subnet of the Cisco IMC.
- Gateway—Enter the gateway address.
- Pref DNS Server—Enter the preferred DNS server address.
- NIC Redundancy—Null.

Step 10 Press **F1** to view the additional settings.

Step 11 In the Additional Settings window, update the following fields:

- Hostname—Enter the Cisco IMC hostname.
- Dynamic DNS—**Disable**.
- Enter the admin password. If you leave the Password field blank, the default password is **password**.

Step 12 Press **F10** to save the settings.

Step 13 Open a browser and enter the following URL:

`https://Cisco IMC_IP_address`

Where *Cisco IMC_IP_address* is the Cisco IMC IP address that you entered in *Step 9*.

Step 14 Log into the Cisco IMC using the credentials that you entered in *Step 7*.

What to do next

Proceed to Configure the Bare Metal Cisco UCS Server.

Configure the Bare Metal Cisco UCS Server

This procedure is specific to the Cisco 12G SAS Modular Raid Controller. For any other Raid controller please refer to the Cisco UCS Servers RAID Guide.

Step 1 Set the local and UTC time zones and set boot options, as follows:

a) From the left sidebar of the Cisco IMC web interface, choose **Chassis > Summary**.
b) Change the time zone to the correct *local* time zone.
c) Launch KVM and connect to the server.
d) Reset the server (warm boot).
e) When prompted, press F2 to enter CMOS.
f) Change the time to the current UTC time (not the local time) and press F10 to save your change.
g) **For UCS C220 M4 devices only:**Click the **Boot Options** tab. Enable **UEFI Boot options**, and then choose **Bus PCI RAID Adapter** for Boot Option #1.
h) Reboot the host.
i) Reboot Cisco IMC and log in again.
j) Check that the time is correct in **Chassis > Summary**.

Step 2 From the left sidebar of the Cisco IMC web interface, choose **Storage > Cisco 12G SAS Modular Raid Controller (SLOT-HBA)**.

Step 3 In the Cisco 12G SAS Modular Raid Controller (SLOT-HBA) pane, click the **Controller Info** tab.

Step 4 Under Physical Drive Info, make sure that boot drive is not set to true for any physical drives.

Step 5 In the Actions area, click **Create Virtual Drive** from the **Unused Physical Drives** link.

Step 6 In the Create Virtual Drive from Unused Physical Drives window, choose **10** from the RAID Level drop-down list.

Step 7 In the Create Drive Groups area, select the physical drives listed under the Physical Drives area, then add them to the Drive Groups.

Step 8 In the Virtual Drive Properties area, choose **Write Back Good BBU** from the Write Policy drop-down list.

Step 9 Complete the required fields, then click **Create Virtual Drive**.

Step 10 Click the **Virtual Drive Info** tab.

Step 11 Click **Initialize**. A popup window is displayed.

Step 12 Click **Initialize VD** and select **Full Initialize**. Wait for the operation to complete (between 30 and 60 minutes).

Step 13 Follow the steps below to enable Auto-Negotiation to speed up the installation:

1. From the left sidebar, click the **Admin** tab.
2. Click **Network**.
3. In the Network pane, click the **Network Settings** tab.
4. In the Port Properties area, check the **Auto Negotiation** check box.
5. Click **Save Changes**.

Step 14 From the left sidebar, click the **Admin** tab.

Step 15 In the Utilities pane, click the **Actions** area, then click **Reboot Cisco IMC**.

Step 16 Click **OK**.

Step 17 Press **F10** to save and exit.

The system is now prepared to boot from RAID. (The first boot, however, must be done from a remote virtual CD/DVD which is mapped to the ISO image. That process is described in Install Cisco EPN Manager from an ISO Image.)

What to do next

Proceed to Install Cisco EPN Manager from an ISO Image.

Install Cisco EPN Manager from an ISO Image

Step 1 Power up the Cisco UCS Server.

Step 2 Log into the Cisco IMC Server using the credentials you entered when configuring the IMC server. See Configure the Cisco IMC Server.

Step 3 Choose **Chassis > Summary**, then click **Launch KVM** to open the console (in a separate window).

Note Make sure that you are using the Java version of KVM and not the HTML version as the HTML version might be interrupted by the browser causing remote media installations to fail.

Step 4 In the KVM Console window, choose **Virtual Media > Activate Virtual Devices**. A popup window is displayed.

Step 5 Click the **Accept this Session** radio button, then click **Apply**.

Step 6 In the KVM Console window, choose **Virtual Media > Map CD/DVD**.

Step 7 In the Virtual Media - Map CD/DVD window, select the ISO file, then click **Map Device**.

Step 8 In the KVM Console window, choose **Virtual Media** and verify that the **ISO filename .iso Mapped to CD/DVD** option is displayed.

Step 9 Reboot the server by choosing **Power > Reset System** (warm boot).

Step 10 Enter the boot menu by pressing **F6**.

Step 11 From the boot device selection window, select **Cisco vKVM-Mapped vDVD1.22**, then press **Enter**.

Step 12 For the boot option, enter **1** for Keyboard/Monitor or **2** for Serial Console, then press **Enter**. The Cisco EPN Manager installer extracts the content.

You can monitor the progress in the KVM Console by selecting **Tools > Stats**. When the amount transferred is approximately 5 GB, the operation is complete.

Note Do not monitor the screen for install progress because this will cause the transfer to be 50-60% slower. Rather allow the screen to go sleep and display "No Signal".

Step 13 After the extraction is complete, at the localhost login prompt, enter **setup**.

Step 14 Go to *Step 3* in Install Cisco EPN Manager on the Server to complete the installation.

Post-Installation Tasks

Step 1 As the Root user, run the **ncs status** command and make sure that all the processes are up and running.

Step 2 Run the following command to to synchronize all files with the local time on the server:

```
find /opt/CSCOlumos/updates/ -mmin -0 -print0 | xargs -0 touch -t $(($(date +%Y%m%d%H%M)-6))
```

Uninstall Cisco EPN Manager

- Uninstall Cisco EPN Manager (OVA/VM)
- Uninstall Cisco EPN Manager (ISO/Bare Metal)

Uninstall Cisco EPN Manager (OVA/VM)

Before You Begin

Perform a backup. Uninstalling Cisco EPN Manager using the following method will permanently delete all your data on the server, including server settings and local backups. You cannot restore your data unless you have a remote backup. Refer to the backup topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Step 1 In the VMware vSphere client, right-click the Cisco EPN Manager virtual machine.

Step 2 Power off the virtual machine.

Step 3 Click **Delete from Disk** to remove the Cisco EPN Manager virtual appliance.

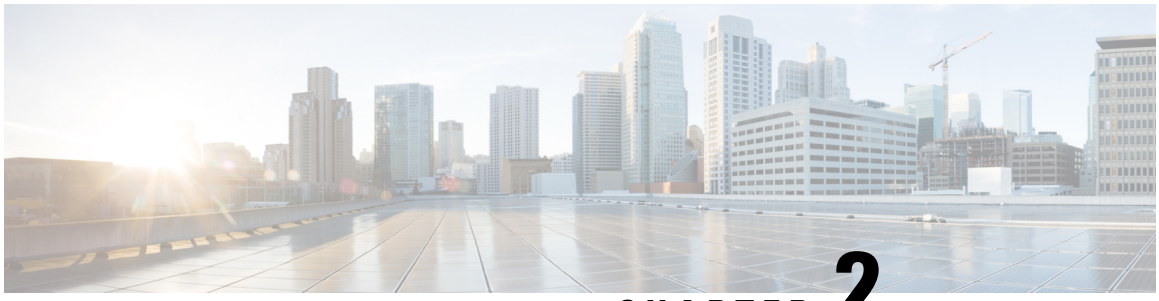
Uninstall Cisco EPN Manager (ISO/Bare Metal)

Before You Begin

Make sure you have backed up your current data. See the backup and restore topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

To ensure information security, Cisco recommends you use either of the following methods to remove Cisco EPN Manager from the Cisco UCS server:

- Digital file shredding—Use the digital file shredding utility to securely delete the files and clean the disk space.
- RAID secure deletion—If you are using a RAID system, use the RAID features to securely delete the files.



CHAPTER 2

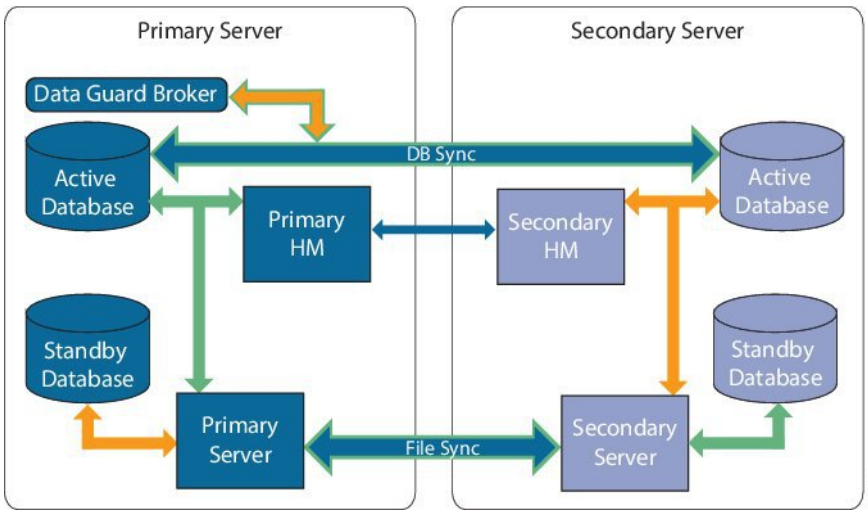
Cisco EPN Manager 3.0 High Availability Installation

This chapter provides information and procedures for installing Cisco EPN Manager in a high availability environment:

High Availability Overview

The Cisco EPN Manager high availability (HA) system ensures continued system operation in case of failure. HA uses a pair of linked, synchronized Cisco EPN Manager servers to minimize or eliminate the impact of application or hardware failures that may take place on either server.

The following figure shows the main components and process flows for a high availability deployment.



A high availability deployment consists of a primary and a secondary server with Health Monitor (HM) instances (running as application processes) on both servers. When the primary server fails (due to a problem or because it is manually stopped), the secondary server takes over and manages the network while you restore access to the primary server. If the deployment is configured for automatic failover, the secondary server takes over the active role within two to three minutes after the primary server failure.

When issues on the primary server are resolved and the server is in a running state, it remains in standby mode and begins syncing its data with the active secondary server. When failback is triggered, the primary server again takes over the active role. This role switching between the primary and secondary servers generally takes approximately two to three minutes unless the primary server was reinstalled after failure, in which case it would take longer (based on the size of your setup).

For more information about HA, see the High Availability sections in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

High Availability Deployment Considerations

High Availability Deployment Models

Cisco EPN Manager supports the following High Availability (HA) deployment models.

HA Deployment Model	Primary and Secondary Server Location	Example:
Local	On the same subnet (Layer 2 proximity)	Servers located in same data center
Campus	Different subnets connected via LAN	Servers located in same campus, city, state, or province
Remote	Different subnets connected via WAN	Servers are geographically dispersed

Consider the following factors when deciding whether to use the Local, Campus, or Remote HA deployment model:

- Exposure to disaster—The more distributed the deployment model, the less risk to the business as a result of a natural disaster. Remote HA deployments are least likely to be affected by natural disaster, allowing for a less complex and costly business continuity model. Local HA deployments are most vulnerable to disaster because of server co-location.
- Whether you can use a virtual IP address—Only Local HA deployments can use virtual IP addresses. A virtual IP address is a single IP address that will always point to the active server, even after a failover and failback. It also allows both the primary and secondary servers to share a common management IP address.
- Bandwidth/latency—Bandwidth would be highest and latency would be lowest in Local HA deployments because the primary and secondary servers are connected by short network links that have high bandwidth and low latency. Campus HA deployments may have lower bandwidth and higher latency than Local HA deployments. Remote HA deployments have the least bandwidth and the highest latency.

- Administration—HA administration is simplest for Local HA deployments, with increasing complexity for Campus and Remote HA deployments. Remote HA deployments will require administrative remedying.
- Configuration of device event forwarding—Configuring event forwarding can be simplest with Local HA deployments because you can use a virtual IP address, and then configure your devices to forward events to that single virtual IP address. Without a virtual IP address, you must configure your devices to forward events to both the primary and secondary servers.

For more details about HA, see the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Understand High Availability Limitations

The Cisco EPN Manager HA system is subject to the following limiting factors (this applies to all HA deployment models):

- The HA system requires at least 255 Mbps of network bandwidth to handle HA operations (the ideal is 977 Mbps). These operations include (but are not restricted to) HA registration, database and file synchronization, and triggering failback. Because Cisco EPN Manager uses a single physical port for all its networking needs, there can be occurrences of insufficient bandwidth which in turn will affect HA performance.
- The HA system requires low latency (less than 100 msecs) across network links between the primary and secondary servers. Irrespective of the physical proximity of these two servers, high latency on these links can affect how Cisco EPN Manager maintains sessions between the primary and secondary servers. This is because larger databases require more synchronization transactions which require lower latency and higher bandwidth. If you are managing a relatively small network using Cisco EPN Manager, your database would be smaller and therefore, HA might work with a higher network latency and less bandwidth.
- HA performance is always sensitive to the network throughput delivered by the network that connects the primary and secondary servers. This restriction applies (to some degree) to all of the deployment models. For example, in a geographically dispersed deployment, a Remote HA deployment is more likely to have problems due to low bandwidth and high latency. However, if Local and Campus HA deployments are not properly configured, they are highly susceptible to problems with latency that result from bandwidth limitations on high-usage networks.

For assistance in determining whether your network is suitable for any of the HA variations, please contact your Cisco representative.

Consider Whether You Can Use Virtual Addresses

Using virtual IP addresses in a Local HA deployment setup gives your users the ability to connect to the active server using a single IP address or web URL without having to know which server is actually active. Virtual IP addresses also allow both servers to share a common management IP address. During normal operation, the virtual IP address points to the primary server. If a failover occurs, the virtual IP address automatically points to the secondary server. When failback occurs, the virtual IP address automatically switches back to the primary server.

To use a virtual IP addresses, the following IP addresses must be on the same subnet:

- The virtual IP address
- The IP addresses of the primary and secondary servers
- The IP address of the gateway configured on both primary and secondary servers

The following example illustrates how virtual, primary, and secondary IP addresses should be assigned with respect to each other. If the primary and secondary servers have the following IP address assignments within the given subnet, the virtual IP address for both servers can be assigned as follows:

- Subnet mask: 255.255.255.224 (/32)
- Primary server IP address: 10.10.101.1
- Secondary server IP address: 10.10.101.2
- Virtual IP address: 10.10.101.[3-30] e.g., 10.10.101.3. Note that the virtual IP address can be any of a range of addresses that are valid for the given subnet mask.

If you do not use a virtual IP address, you must configure your devices to forward events to both the primary and secondary servers (for example, by forwarding them to a given subnet or range of IP addresses that includes both the primary and secondary server). To reduce (or eliminate) the chance of losing data, you must configure device event forwarding before a failover occurs. You do not need to make any changes to the secondary server during installation; simply provision the primary and secondary servers with their individual IP addresses.

Whether your HA deployment uses a single IP address or not, users should always connect to the Cisco EPN Manager web GUI using the active server IP address/URL.

Best Practices if Firewall is Used Between Primary and Secondary Servers

Firewalls between the primary and secondary servers should be configured to avoid short timeouts for TCP packets to allow enough time for HA registration and other processes.

Following is the procedure for changing the Oracle and OS timeouts, if necessary. Use this procedure if the failback operation fails repeatedly.

Before you Begin

Back up the files specified in the procedure below.

Note This procedure must be performed on both primary and secondary servers.

Step 1 Open the following file:

/opt/oracle/base/product/12.1.0/dbhome_1/network/admin/sqlnet.ora

Step 2 Add the following parameters:

```
SQLNET.EXPIRE_TIME=2
DISABLE_OOB=on
SQLNET.INBOUND_CONNECT_TIMEOUT=600
```

Step 3 Open the following file:

/opt/CSCOlumos/bin/ha_dgmgrl.sh

Step 4 Add the following line under the register() function:

```
edit database $1 set property NetTimeout=1000
```

Following is an example excerpt of the file with the relevant line in bold:

```
connect $4/$5@$3
remove configuration;
create configuration $DGMGRL_CONFIG_NAME as primary database is $1 connect identifier is $1;
edit database $1 set property NetTimeout=1000
;
add database $2 as connect identifier is $2 maintained as physical;
enable configuration;
```

Step 5 Open the following file:

/etc/sysctl.conf

Add the following commands to the end of the file:

```
net.ipv4.tcp_keepalive_time = 80
net.ipv4.tcp_keepalive_probes = 7
net.ipv4.tcp_keepalive_intvl = 10
```

Step 6 Run the following command from the root shell:

```
sysctl -system
```

Prerequisites for High Availability Installations

The following prerequisites must be met before installing Cisco EPN Manager in a high availability deployment:

- Make sure that your hardware and software meet the requirements listed in the relevant prerequisites topic:
  - OVA/VM Requirements.
  - Bare Metal Requirements for Remote High Availability Deployments, on page 7.
- Make sure the secondary server is configured as follows:
  - The secondary server's hardware and software specifications must be the same as those of the primary server. For example, if you installed Cisco EPN Manager on the primary server and specified the Professional system size, your secondary server must also be installed using the Professional system size, and must meet all requirements for Professional-size servers in System Requirements.
  - The secondary server must be running the same software level as the primary server (including the patch level).
  - If you plan to use a virtual IP address for a Local HA deployment, the virtual IP address, primary, and secondary servers must be on the same subnet. The gateway on the primary and secondary servers must also reside on the same subnet.
- If there is a firewall between the primary and secondary servers, there must be permission from the firewall for the ports used by HA. The ports are listed in Ports Used by Cisco EPN Manager.
- Prepare the following information which you will need to enter during the installation:
  - The IPv4 IP address or host name of the secondary server (if you are not using a virtual IP address). You will need it when configuring HA on the primary server.
  - The virtual IPv4 and IPv6 (if used) IP addresses you want to use for both servers (if you plan to use a virtual IP address).

- The password you want to use for the HA authentication key. This password was provided by the user during the installation of the secondary server. It will be used to authenticate communications between the primary and secondary servers. You will need to enter it when you configure HA—that is, when you register the secondary server on the primary server (also called *pairing* the servers). Finally, you will need it to log in to the secondary server's Health Monitor page.
- A Cisco EPN Manager web GUI user ID with Administration privileges on the primary server. You will also need the user's password.
- A valid email address to which HA notifications can be sent.

Install Cisco EPN Manager 3.0 in a High Availability Deployment

The procedure in this section is for a fresh installation of the product in a high availability environment. If you are upgrading to Cisco EPN Manager 3.0 from a previous version, see Upgrade to Cisco EPN Manager 3.0 (High Availability), on page 38.

Before You Begin

Make sure your servers meet the requirements listed in Prerequisites for High Availability Installations.

Step 1 Install Cisco EPN Manager on the primary server as described in Install Cisco EPN Manager 3.0 (No HA), on page 16.

Step 2 Install Cisco EPN Manager on the secondary server as described in Install Cisco EPN Manager 3.0 (No HA), on page 16.

Step 3 When you are prompted to choose whether you want this newly-installed server to act as a secondary failback server in an HA implementation, enter **`yes`**.

Step 4 Enter a password which will be used as the *HA authentication key* for communication between the primary and secondary servers. You will need this key to configure HA. (During normal operation, you will need to enter the HA authentication key to log in to the secondary server's Health Monitor page.)

Step 5 Enter the password again to confirm.

Step 6 Enter **`Y`** to confirm that you want to install this server as a secondary server. When the installation is complete, the VM (OVA/VM) or Cisco UCS server (ISO/bare metal) will reboot.

Step 7 Log in using the Cisco EPN Manager CLI admin username and password you specified during the installation.

Step 8 Verify that all the processes are running on the secondary server using the **ncs status** command. Ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 9 Make sure all devices are configured to forward events (syslogs, traps, and TL1 messages) to both servers (or the virtual IP address, if you are using one).

Note If you do not perform this step *before* registering the secondary server on the primary server and a failover occurs, you may lose some data.

Step 10 Configure HA by registering the secondary server on the primary server. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Check Readiness for HA Configuration

During the HA configuration, other environmental parameters related to HA like system specification, network configuration and bandwidth between the servers determine the HA configuration.

15 checks are run in the system to ensure the HA configuration completion without any error or failure. The checklist name and the corresponding status with recommendations if any, will be displayed when you run the Check Readiness feature.

Note The **Check Readiness** does not block the HA configuration. You can configure HA even if some of the checks do not pass.

To check readiness for HA configuration, follow these steps:

Step 1 Log in to Cisco EPN Manager with a user ID and password that has administrator privileges.

Step 2 From the menu, select **Administration** > **Settings** > **High Availability**. Cisco EPN Manager displays the HA status page.

Step 3 Select **HA Configuration**.

Step 4 Provide the secondary server IP address in the **Secondary Server** field and secondary Authentication Key **Authentication Key** field .

Step 5 Click **Check Readiness**.

A pop up window with the system specifications and other parameters will be displayed. The screen will show the Checklist Item name, Status, Impact and Recommendation details.

Below, is the list of checklist test name and the description displayed for Check Readiness:

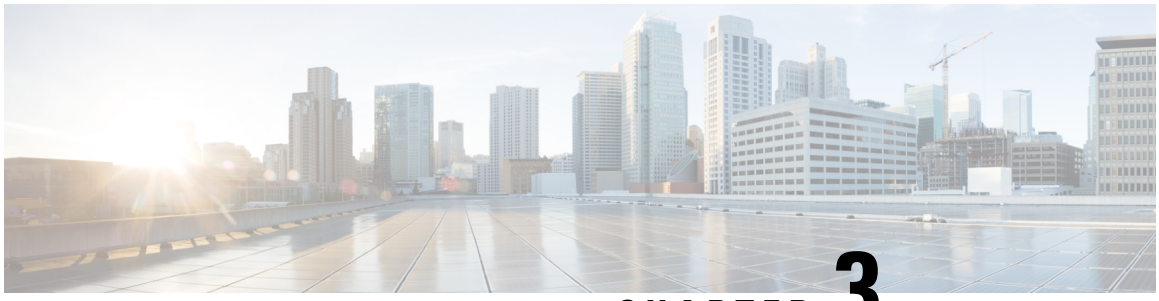
Table 3: Checklist name and description

Checklist Test Name	Test Description
SYSTEM - CHECK CPU COUNT	Checks the CPU count in both the primary and secondary servers. The CPU count in both servers must meet the requirements.
SYSTEM - CHECK DISK IOPS	Checks the disk speed in both the primary and secondary servers. The minimum expected disk speed is 200 MBps.
SYSTEM - CHECK RAM SIZE	Checks the RAM size of both the primary and secondary servers. The RAM size of both servers must meet the requirements.
SYSTEM - CHECK DISK SIZE	Checks the disk size of both the primary and secondary servers. The disk size of both servers must meet the requirements.

SYSTEM - CHECK SERVER PING REACHABILITY	Checks that the primary server can reach the secondary server through ping.
SYSTEM - CHECK OS COMPATABILITY	Checks that the primary server and secondary servers have the same OS version.
SYSTEM - HEALTH MONITOR STATUS	Checks whether the health monitor process is running in both the primary and secondary servers.
NETWORK - CHECK NETWORK INTERFACE BANDWIDTH	Checks if the speed of interface eth0 matches the recommended 100 Mbps in both primary and secondary severs. This test will not measure network bandwidth by transmitting data between primary and secondary server.
NETWORK - CHECK FIREWALL FOR DATABASE PORT ACCESSIBILITY	Checks if the database port 1522 is open in the system firewall. If the port is disabled, the test will grant permission for 1522 in the iptables list.
DATABASE - CHECK ONLINE STATUS	Checks if the database files status is online and accessible in both primary and secondary servers.
DATABASE - CHECK MEMORY TARGET	Checks for "/dev/shm" database memory target size for HA setup.
DATABASE - LISTENER STATUS	Checks if the database listeners are up and running in both primary and secondary servers. If there is a failure the test will attempt to start the listener and report the status.
DATABASE - CHECK LISTENER CONFIG CORRUPTION	Checks if all the database instances exist under database listener configuration file "listener.ora"
DATABASE - CHECK TNS CONFIG CORRUPTION	Checks if all the “WCS” instances exist under database TNS listener configuration file “tnsnames.ora"
DATABASE - TNS REACHABILITY STATUS	Checks if TNSPING is successful in both primary and secondary server.

Step 6 Once the check is completed for all the parameters, check their status and click **Clear** to close the window.

Note Failback and failover events during **Check Readiness** are forwarded to the Alarms and Events page. Configuration failure events are not present in the Alarms and Events list.



CHAPTER 3

Upgrade to Cisco EPN Manager 3.0

If you are already working with Cisco EPN Manager, you can upgrade to Cisco EPN Manager 3.0 by following one of the Valid Upgrade Paths, on page 33.

There are two upgrade methods:

- Backup-restore upgrade (recommended)—Involves backing up all data from the currently installed version of Cisco EPN Manager, then installing Cisco EPN Manager 3.0 on a new server, then restoring the backed up data to the new Cisco EPN Manager 3.0 server.
- In-place upgrade—Involves upgrading the application to the latest version on the server on which you are currently running Cisco EPN Manager.

This chapter provides instructions for upgrading to Cisco EPN Manager 3.0 using both of these methods.

The following topics provide prerequisites and procedures for upgrading in standard and high availability deployments:

Valid Upgrade Paths

The following table lists the valid paths for installing/upgrading to Cisco EPN Manager 3.0 from previous versions.

Current Cisco EPN Manager Version	Upgrade Path to Cisco EPN Manager 3.0:
Cisco EPN Manager 2.2	**Cisco EPN Manager 2.2.0.4 (latest point patch) > 3.0**
Cisco EPN Manager 2.2.1	**Cisco EPN Manager 2.2.1.3 (latest point patch) > 3.0**

In-place upgrade to Cisco EPN Manager 3.0 is possible from the following versions:

Current Cisco EPN Manager Version	Upgrade Path to Cisco EPN Manager 3.0:
Cisco EPN Manager 2.2.1	**Cisco EPN Manager 2.2.1.3 (latest point patch) > 3.0**

See the relevant installation guide for installation prerequisites and procedures for Cisco EPN Manager versions.

For point patch installation instructions, see the readme file supplied with the patch file on the on the Software Download site on Cisco.com.

Prerequisites for Upgrading to Cisco EPN Manager 3.0

Before starting the upgrade:

1. Ensure that you have followed the relevant upgrade path based on your current version of Cisco EPN Manager. See Valid Upgrade Paths, on page 33.
2. Ensure that your deployment meets the requirements in the relevant prerequisites topic:
   - Prerequisites for OVA/VM Installations. For OVA/VM deployments, the upgrade is run from the vmWare vSphere client.
   - Prerequisites for ISO/Bare Metal Installations. For ISO/bare metal deployments, the upgrade is run from the Cisco IMC server.
3. Remove any devices running uncertified software versions from Cisco EPN Manager. This step is not mandatory but highly recommended.
4. Back up your data. See Create a Copy of Your Data.
5. Ensure that no backups are running.
6. Ensure that SCP is enabled on your client machine and the required ports are open (see Ports Used by Cisco EPN Manager). You will need to use SCP to copy files from your client machine to the Cisco EPN Manager server.
7. Copy any gpg files located in /localdisk/defaultRepo to an external repository and then delete them from this folder.

Create a Copy of Your Data

Use one or both of the following options to create a copy of your current data:

1. Back up your data to a remote repository. Refer to the backup topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide . If necessary, you can revert to the previous version by restoring the data. See Revert to the Previous Version using Data Restore.
2. If you are using a virtual machine (VM), take a base snapshot of the VM. Depending on whether you have a high availability (HA) environment or not, follow one of the procedures below. If necessary, you can revert to the previous version using the VM snapshot to restore the data. See Revert to the Previous Version Using the VM Snapshot.

Take a Base Snapshot of the VM (no HA)

Step 1 Stop Cisco EPN Manager.

```
ncs stop
```

Step 2 Suspend the VM and take a VM snapshot. Consult your system administrator for assistance, if necessary.

Step 3 Start Cisco EPN Manager.

```
ncs start
```

Take a Base Snapshot of the VM (HA)

Step 1 Remove the HA configuration:

1. Log into the Cisco EPN Manager web GUI as a user with Administrator privileges.
2. From the left sidebar, choose **Administration** > **Settings** > **High Availability**.
3. Click **HA Configuration** on the left.
4. Click **Remove**.
5. When the remove operation completes, confirm that the Configuration Mode field displays **HA Not Configured**.

Step 2 Stop Cisco EPN Manager on the primary and the secondary servers (while logged in as the Cisco EPN Manager CLI admin user.)

```
ncs stop
```

Step 3 Pause the VM and take a VM snapshot on both the primary and secondary servers. Consult your system administrator for assistance, if necessary.

Step 4 Start Cisco EPN Manager on the primary and secondary servers.

```
ncs start
```

Upgrade to Cisco EPN Manager 3.0 (No HA)

These topics explain how to upgrade to Cisco EPN Manager 3.0 from an earlier version of Cisco EPN Manager in a standard deployment (no high availability).

- In-Place Upgrade
- Backup-Restore Upgrade
- Post-Upgrade Tasks

If you are performing an upgrade in a high availability deployment, see Upgrade to Cisco EPN Manager 3.0 (High Availability), on page 38.

In-Place Upgrade

Note Run this upgrade:

In VM: From the VM Console in ESXi Host

In Bare Metal: From KVM Console

what does this mean

In-place upgrade involves upgrading the application to the latest version on the server on which you are currently running Cisco EPN Manager.

In-place upgrade involves the following basic steps which are explained in detail in the procedure below:

1. Download the upgrade image from Cisco.com to your client machine.
2. Copy the files from your client machine to the Cisco EPN Manager server.
3. Perform the upgrade.
4. Perform the post-upgrade licensing, authentication, and web GUI tasks described in Post-Upgrade Tasks.

Before You Begin

1. Complete the tasks in Prerequisites for Upgrading to Cisco EPN Manager 3.0, on page 34.

To upgrade:

Step 1 From the Software Download site on Cisco.com , locate and download the upgrade image to your client machine. The file will have the prefix **CEPNM-upgrade** and the suffix **.tar.gz**. The numbers in the filename may not align to the current Cisco EPN Manager version, so be sure to check the file description.

Step 2 After the download completes, compare the upgrade image's size on the Software Download site with its size on your client machine to make sure that the full file was downloaded. On the Software Download site, hover your mouse cursor over the upgrade image to view its MD5 Checksum size in a popup window, then compare it against the size on your client machine.

Step 3 Make sure the /localdisk/defaultRepo directory has enough space to copy the files.

1. Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
2. Log in as the as Linux CLI root user as described in Log In and Out as the Linux CLI Users.
3. Move all files from /localdisk/defaultRepo to a remote repository. Ensure that only the upgrade tar file is placed in /localdisk/defaultRepo

```
df -h /localdisk/defaultRepo
```

Step 4 Use SCP to retrieve the files from your client machine and copy them to the Cisco EPN Manager server's default local repository (/localdisk/defaultRepo). Run this command as the Linux CLI root user.

```
scp clientUsername@clientIP:/fullpath-to-file /localdisk/defaultRepo
```

Where:

- *clientUsername* is your username on the client machine
- *clientIP* is the IP address of the client machine to which you downloaded the files in Step 1
- *fullpath-to-file* is the full pathname of the upgrade file on the client machine

For example (the following command is one line):

```
scp jsmith@123.456.789.101:/temp/CEPNM-Upgrade-2.1.X_to_2.2.tar.gz /localdisk/defaultRepo
```

Step 5 After the file is transferred to the Cisco EPN Manager server, compare the MD5 Checksum size of the Cisco EPN Manager upgrade image against the value in Step 2 to ensure it has not been damaged.

Step 6 Log out as the Linux CLI root user.

```
su admin
```

Step 7 Stop the server.

```
ncs stop
```

Step 8 From the vmWare vSphere client (OVA) or the Cisco IMC server (Bare Metal): Upgrade the Cisco EPN Manager software using the upgrade file that is located in /localdisk/defaultRepo.

```
application upgrade filename defaultRepo
```

Where *filename* is the upgrade file located in /localdisk/defaultRepo. For example:

```
application upgrade CEPNM-Upgrade-2.2.X_to_3.0-xxx.tar.gz
```

Step 9 The script will ask you if you want to save the running ADE-OS configuration, and if you want to proceed with the upgrade. Answer **yes** to both questions.

```
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Please ensure you have a backup of the system before proceeding.Proceed with the application install
 ? (yes/no) [yes] ? yes
```

Step 10 Wait for the upgrade to complete and for Cisco EPN Manager to restart. This could take a few hours.

What to do next

Perform the tasks in Post-Upgrade Tasks.

Backup-Restore Upgrade

Backup-restore upgrade involves backing up all data from the currently installed version of Cisco EPN Manager, then installing Cisco EPN Manager 3.0 on a new server, then restoring the backed up data to the new Cisco EPN Manager 3.0 server. This is the recommended upgrade method.

Before You Begin

- Make sure you have completed the tasks in Prerequisites for Upgrading to Cisco EPN Manager 3.0, on page 34.
- Make sure the new server has the same hardware specifications as the server from which the backup was taken.
- Note the location of the remote backup repository used by the old server. You will need it to configure the same backup location on the new server.

Step 1 On the new server, install Cisco EPN Manager 3.0 by following the steps in Install Cisco EPN Manager 3.0 (No HA), on page 16.

Step 2 Configure the new server to use the same remote backup repository as the old server, as explained in the remote backup repository topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Step 3 Restore the backup in the remote repository to the new server, as explained in the restore backup topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

What to do next

Perform the tasks in Post-Upgrade Tasks.

Upgrade to Cisco EPN Manager 3.0 (High Availability)

The following topics provide procedures for upgrading to Cisco EPN Manager 3.0 in a high availability deployment:

- In-Place Upgrade (High Availability)
- Backup-Restore Upgrade (High Availability)

Note High availability will not be functional until the upgrade is complete.

In-Place Upgrade (High Availability)

In-place upgrade in an HA environment involves the following basic steps which are explained in detail in the procedure below:

1. Remove the HA configuration.
2. Download the upgrade image from Cisco.com to your client machine.
3. Copy the file from your client machine to the Cisco EPN Manager primary server.
4. Perform the upgrade on the primary server.
5. Install Cisco EPN Manager 3.0 on the secondary server.
6. Perform the post-upgrade licensing, authentication, and web GUI tasks described in Post-Upgrade Tasks.
7. Reconfigure HA by pairing the primary and secondary servers.

Before You Begin

Ensure that:

- Your deployment meets the general HA requirements listed in Prerequisites for High Availability Installations.
- Your deployment meets the upgrade-specific requirements listed in Prerequisites for Upgrading to Cisco EPN Manager 3.0.
- You have the password (authentication key) that was created when HA was enabled. You will need it to perform the Cisco EPN Manager 3.0 installation on the secondary server.

Step 1 On the primary server, note the HA configuration, then remove it.

1. Log into Cisco EPN Manager as a user with Administrator privileges.

2. Choose **Administration > Settings > High Availability**.
3. Make note of the HA configuration. You will need this information to reconfigure HA after the upgrade.
4. Choose **HA Configuration** in the left navigation area, then click **Remove**.
5. Wait for the remove operation to complete.
6. Click **HA Configuration** in the left navigation area and confirm that the Configuration Mode field displays **HA Not Configured**.

Step 2 From the Software Download site on Cisco.com , locate and download the upgrade image to your client machine. The file will have the prefix **CEPNM-upgrade** and the suffix **.tar.gz**. The numbers in the filename may not align to the current Cisco EPN Manager version, so be sure to check the file description.

Step 3 Compare the MD5 Checksum size of the CEPNM upgrade image from the Software Download site against the size on your client machine. On the Software Download site, hover your mouse cursor over the upgrade image to view its size in a popup window, then compare it against the size on your client machine.

Step 4 On the primary server, make sure the /localdisk/defaultRepo directory has enough space to copy the files.

1. Start an SSH session with the primary Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
2. Log in as the as Linux CLI root user as described in Log In and Out as the Linux CLI Users.
3. Move all files from /localdisk/defaultRepo to a remote repository. Ensure that only the upgrade tar file is placed in /localdisk/defaultRepo.

```
df -h /localdisk/defaultRepo
```

Step 5 Use SCP to retrieve the files from your client machine and copy them to the Cisco EPN Manager primary server's default local repository (/localdisk/defaultRepo). You should run this command as the Linux CLI root user.

```
scpclientUsername@clientIP:/fullpath-to-file/localdisk/defaultRepo
```

Where:

- *clientUsername* is your username on the client machine
- *clientIP* is the IP address of the client machine to which you downloaded the files in *Step 2*
- *fullpath-to-file* is the full pathname of the upgrade file on the client machine

For example (the following command is one line):

```
scp jsmith@123.456.789.101:/temp/CEPNM-Upgrade-2.2.X_to_3.0-xxx.tar.gz  /localdisk/defaultRepo
```

Step 6 After the file is transferred to the primary server, compare the MD5 Checksum size of the Cisco EPN Manager upgrade image against the value in *Step 3* to ensure it has not been damaged.

Step 7 On the primary server, log out as the Linux CLI root user.

```
su admin
```

Step 8 Stop the primary server by running the following command:

```
ncs stop
```

Step 9 From the vmWare vSphere client (OVA) or the Cisco IMC server (Bare Metal):Upgrade the primary server using the upgrade file that is located in /localdisk/defaultRepo.

```
application upgrade filename defaultRepo
```

Where *filename* is the upgrade file located in /localdisk/defaultRepo. For example:

```
application upgrade CEPNM-Upgrade-2.2.X_to_3.0-xxx.tar.gz defaultRepo
```

Step 10 The script will ask you if you want to save the running ADE-OS configuration, and if you want to proceed with the upgrade. Answer **yes** to both questions.

Save the current ADE-OS running configuration? (yes/no) [yes] ? **yes**

Please ensure you have a backup of the system before proceeding.Proceed with the application install ? (yes/no) [yes] ? **yes**

This step can take 180 minutes or more to complete, depending on the size of the application database. However you can continue with the next step while the upgrade is in progress for the primary server. Once the upgrade is complete, the primary server will be automatically restarted as part of the upgrade.

Step 11 Install Cisco EPN Manager 3.0 on the secondary server (you will perform a fresh installation on this server):

- **OVA/VM installation**—Perform these steps:
  1. Delete the existing VM:
     1. Launch the VMware vSphere client.
     2. Select the VM to be deleted and choose **Shut Down Guest**.
     3. Select the VM again and choose **Delete From Disk**.
     4. Click **Yes** in the displayed confirmation message.
  2. Deploy the OVA from the VMware vSphere Client
  3. Install Cisco EPN Manager on the secondary server. See Install Cisco EPN Manager on the Server

  Note (OVA/VM) If you want to retain the same IP address on the secondary server, you must first remove it from the vmWare vSphere client, then use the original address when you deploy the OVA.

- **ISO/bare metal installation**—Perform the steps in these sections:

  Note The installation procedure provided in these sections is specific to the UCS server type and hardware requirements described in Bare Metal Requirements.

  1. Configure the Bare Metal Cisco UCS Server
  2. Install Cisco EPN Manager on the Server

Step 12 Update the time zone for the Compliance engine.

1. Log into the primary server as the Linux CLI root user (see Log In and Out as the Linux CLI Users).
2. Update the time zone using a soft link (the following command is one line):

```
ln -sf /usr/share/zoneinfo/$(grep ^clock /storedconfig/active/startup-config | cut -d " " -f 3)
 /etc/localtime
```

Step 13 On the primary server:

1. Start the server and then verify that the server is restarted.
2. Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted. Ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM

Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 14 On the secondary server:

1. Verify that the server is restarted.
2. Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted. Ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 15 Perform the post-upgrade tasks on the primary server. See Post-Upgrade Tasks.

Step 16 Once the post upgrade tasks are completed, re-configure HA by registering the secondary server on the primary server. Use the information you saved in *Step 1*. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server, in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Backup-Restore Upgrade (High Availability)

Backup-restore upgrade in an HA environment involves the following basic steps which are explained in detail in the procedure below:

1. Remove HA.
2. Back up your data to a remote repository.
3. Perform a fresh installation of Cisco EPN Manager on both the primary and secondary servers.
4. Restore the backup data on the primary server.
5. Reconfigure HA.

Before You Begin

- Make sure your deployment meets the general HA requirements listed in Prerequisites for High Availability Installations.
- Make sure your deployment meets the upgrade-specific requirements listed in Prerequisites for Upgrading to Cisco EPN Manager 3.0, on page 34.
- Make sure the new server has at least the same hardware specifications as the server from which the backup was taken.
- Note the location of the remote backup repository used by the old server (if applicable). You will need it to configure the same backup location on the new server.
- Make sure that you have the password (authentication key) that was created when HA was enabled. You will need it to perform the Cisco EPN Manager 3.0 installation on the secondary server.

Step 1 On the primary server, remove the High Availability configuration:

1. Log into Cisco EPN Manager as a user with Administrator privileges.
2. Choose **Administration > Settings > High Availability**.
3. Make a note of the HA configuration. You will need this information to reconfigure HA after the upgrade.
4. Choose **HA Configuration** in the left navigation area, then click **Remove**.
5. Wait for the remove operation to complete.

6. Click **HA Configuration** in the left navigation area and confirm that the Configuration Mode field displays **HA Not Configured**.

Step 2 Back up your data to the remote repository. For details, see the topics on backups in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Note If you do not have a remote repository, configure one. See the topics on remote backup repositories in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Step 3 Install Cisco EPN Manager 3.0 on the two new servers as described in Install Cisco EPN Manager 3.0 in a High Availability Deployment, on page 30.

Step 4 Once the installation is completed, configure the new primary server to use the same remote backup repository as the old primary server (which you used in *Step 2*). See the topics on remote backup repositories in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Step 5 On the primary server (only), restore the backup from the remote repository. See the topics on restoring data in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Note You only need to perform the restore operation on the primary server. The secondary server will be synchronized with the primary server when HA is re-enabled.

Step 6 On the primary server:

1. Verify that the server is restarted.
2. Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted. Ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 7 If the **ncs status** output on the primary server lists **Compliance engine is stopped**, do the following:

1. Stop Cisco EPN Manager.

```
ncs stop
```

2. Log in as the Linux CLI root user (see Log In and Out as the Linux CLI Users).
3. Update the time zone using a soft link (the following command is one line):

```
ln -sf /usr/share/zoneinfo/$(grep ^clock /storedconfig/active/startup-config | cut -d " "  -f 3)
 /etc/localtime
```

Step 8 Once the restore is completed, perform the post-upgrade tasks on the primary server. See Post-Upgrade Tasks.

Step 9 Re-configure HA by registering the secondary server on the primary server. Use the information you saved in *Step 1*. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server, in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Post-Upgrade Tasks

- If you are using Cisco Smart Licensing, re-register Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. Refer to the topics that describe managing licenses in the Cisco Evolved Programmable Network Manager User and Administrator Guide .
- Synchronize the inventory of all devices with the database, as follows:
  1. In the Cisco EPN Manager GUI, choose **Monitor > Network Devices**.
  2. Select all devices, then click **Sync**.
- Instruct users to clear the browser cache on all client machines that accessed an older version of Cisco EPN Manager before they try to connect to the upgraded Cisco EPN Manager server.
- If you were using external AAA before the upgrade, configure external authentication again. Refer to the user management topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide.
- During the upgrade, the Cisco EPN Manager home page will be reset to the default home page (Getting Started page). Users can select their own default home page from the Getting Started page or from the Settings menu at the top right of the page.
- Reset all dashboards, as follows:
  1. Open any dashboard.
  2. Click on **Settings** in the top right of the dashboard.
  3. Choose **Manage Dashboards** > **Reset All Dashboards**.

Note The reset dashboard operation removes existing user-defined dashboard tabs and they must be recreated. The reset dashboard operation must be performed after backup/restore or upgrade tasks.

Note The reset dashboard operation must be performed after backup/restore or upgrade tasks.

Revert to the Previous Version of Cisco EPN Manager

This section describes how to go back to the previous version of Cisco EPN Manager after you have installed Cisco EPN Manager, for both high availability and standard environments. This is a manual process—automatic rollback is not supported.

Note You can only revert to a previous version if you created a copy of your data before installing Cisco EPN Manager, as described in Create a Copy of Your Data.

The procedure for reverting to the previous version of Cisco EPN Manager differs depending on which method you used to create a copy of your data.

- If you used the backup facility, see Revert to the Previous Version using Data Restore.

- If you took a VM snapshot, see Revert to the Previous Version Using the VM Snapshot.

Revert to the Previous Version using Data Restore

If you used the backup facility to create a copy of your data, follow one of these procedures to revert to the previous version of Cisco EPN Manager (non-HA or HA).

For non-HA environments, do the following:

1. Reinstall the previous release of Cisco EPN Manager—the release from which you did the backup.
2. Restore the data from the backup. See the topics related to restoring data in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

For HA environments, do the following:

1. Reinstall the previous release of Cisco EPN Manager on the primary and secondary servers—the release from which you did the backup.
2. On the primary server, restore the data from the backup. See the topics related to restoring data in the Cisco Evolved Programmable Network Manager User and Administrator Guide.
3. Configure HA and register the secondary server on the primary server. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Revert to the Previous Version Using the VM Snapshot

If you are using a VM for your installation and you took a VM snapshot prior to the installation, follow one of these procedures to revert to the previous version of Cisco EPN Manager (non-HA or HA).

For non-HA environments, do the following:

1. Shut down the VM.
2. Revert the VM snapshot.
3. Start the VM.
4. Start Cisco EPN Manager.

```
ncs start
```

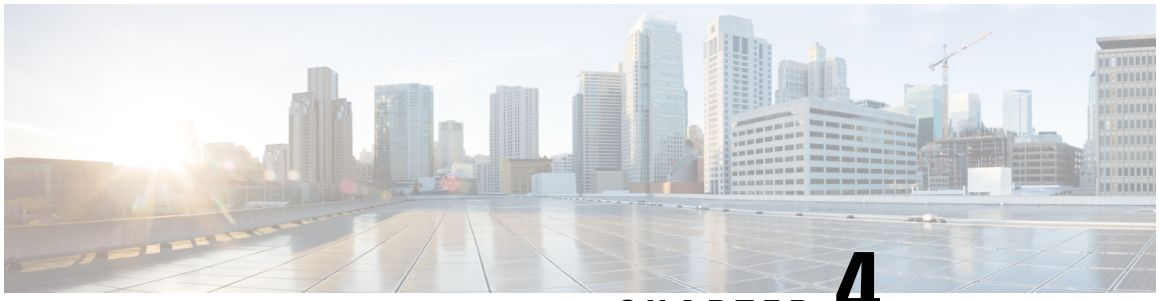
For HA environments, do the following:

1. Shut down the primary and secondary VM servers.
2. Revert the VM snapshot on both servers.
3. Start the primary and secondary VM servers.
4. Start Cisco EPN Manager on the primary server and on the secondary server.

```
ncs start
```

5. Configure HA and register the secondary server on the primary server. The registration process must be performed from the primary server. For more information, see the section on registering the secondary

server on the primary server in the Cisco Evolved Programmable Network Manager User and Administrator Guide.



CHAPTER 4

Install Geo Map Resource Files for Offline Use

The network can be visualized on a topology map or on a geographical map (geo map). The geo map enables you to position your network devices on a world map and monitor them within their geographical context.

To display the geo map in the GUI, the system is set up by default to get the map tiles from a specific Mapbox URL through a direct Internet connection from the client or via the EPN Manager server which acts as a proxy. If you do not have an Internet connection, you must install the map resources locally and specify that you want the system to use the local map resources (i.e., offline use).

The topics below explain how to download and install geo maps for offline use in both HA and non-HA environments.

Note Geo map compressed files are very large. We recommend you save the files to a remote repository.

Install Geo Map Resource Files (Standard Deployment)

Installing geo map resource files for offline use in a standard environment (no high availability) involves the following steps:

1. Place the Geo Map Resource Files on the Cisco EPN Manager Server.
2. Install the Geo Map Resource Files on the Cisco EPN Manager Server .
3. Configure the Cisco EPN Manager Server to Use the Installed Map Resources .
4. Verify that the Geo Maps Files Were Installed Successfully.

Place the Geo Map Resource Files on the Cisco EPN Manager Server

Before You Begin

- If you plan to use a remote repository (because geo map files are very large), make sure a remote repository has been configured. For more information, refer to the topics on using remote FTP backup repositories in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

- Make sure SCP is enabled on your client machine and the required ports are open (see Ports Used by Cisco EPN Manager).

This procedure shows you how to download and copy the geo map resources to the default local repository on the Cisco EPN Manager server.

Step 1 Download the geo map compressed files to a client machine.

1. Go to the Software Download site on Cisco.com .
2. Navigate to the files by choosing **All Releases > 3.0**.
3. Identify the map you want to download and click **Download**.
4. Follow the instructions to save the file to the client machine.

Step 2 Copy the geo map compressed files from the local machine to the Cisco EPN Manager server's default local repository (/localdisk/defaultRepo) by following the procedure in Log In and Out as the Linux CLI Users.

In the following example, the Russia geo map file was downloaded to a /temp directory on the client machine. The user has logged into the Cisco EPN Manager server as the Linux CLI admin user and is retrieving the file from the client machine and copying it to /localdisk/defaultRepo on the server:

```
scp joesmith@123.456.789.101:/temp/Russia_GeoMap_CEPNM_3_0_0-bundle.tar.gz /localdisk/defaultRepo
```

What to do next

Install the geo map files as described in Install the Geo Map Resource Files on the Cisco EPN Manager Server .

Install the Geo Map Resource Files on the Cisco EPN Manager Server

Before You Begin

The installation process will extract the geo map files and install them in /opt/CSCOlumos/resources/offline_geo. To avoid storage constraints, consider mounting additional storage on the directory by editing the /etc/fstab file after logging in as a Linux CLI admin user (see Log In and Out as the Linux CLI Users). If you have high availability and need to mount additional storage, be sure to edit the /etc/fstab file on both the primary and secondary servers.

Step 1 Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.

Step 2 Install the geo map resource file that is located in /localdisk/defaultRepo.

Example:

```
application install filename defaultRepo
```

Where *filename* is the geo map resource file located in /localdisk/defaultRepo (this is the file you copied in Place the Geo Map Resource Files on the Cisco EPN Manager Server). For example:

Example:

```
application install Russia_GeoMap_CEPNM_3_0_0-bundle.tar.gz defaultRepo
```

```
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Please ensure you have a backup of the system before proceeding.Proceed with the application install
 ? (yes/no) [yes] ? yes
```

The installation takes a few minutes to complete depending on the size of the map resources.

What to do next

Configure Cisco EPN Manager to use the installed geo map files, as described in Configure the Cisco EPN Manager Server to Use the Installed Map Resources .

Configure the Cisco EPN Manager Server to Use the Installed Map Resources

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Maps** > **Network Topology**.

Step 2 Check **Enable Geo Maps**.

Step 3 Choose **Installed Map Resources** from the Map Provider drop-down list.

Step 4 Click **Save**.

You do not have to restart the Cisco EPN Manager server to apply your changes. A notification message informs you that the system is now working with the installed map resources.

What to do next

Verify that the geo map files have been installed, as described in Verify that the Geo Maps Files Were Installed Successfully.

Verify that the Geo Maps Files Were Installed Successfully

After installing the geo map files and configuring the system to use these geo map files, check that they have been successfully installed and that they are being displayed in the GUI.

Step 1 Verify that a directory named geoMaps was created under /opt/CSCOlumos/resources/offline_geo:
ls/opt/CSCOlumos/resources/offline_geogeoMaps

Step 2 Check that the map is being displayed in the GUI:

1. Log in to the Cisco EPN Manager web GUI as a user with Administrator privileges.
2. From the left sidebar menu, choose **Maps** > **Topology Maps** > **Network Topology**.
3. Click the Geographical Map icon at the top right of the topology window to display the geo map.
4. Verify that the desired map is displayed. For example, if you installed the map of Russia, it should be displayed.

Install Geo Map Resource Files (High Availability Deployment)

For a high availability environment, you must install the offline map resources on both the primary and the secondary servers.

Note If a failure occurs on the primary server that requires you to reinstall Cisco EPN Manager on the primary server, you must reinstall the geo map resources on the primary server and restart the server.

Follow this workflow to install geo map files in a high availability deployment:

Step 1 Place the geo map files on the primary server and on the secondary server, as described in Place the Geo Map Resource Files on the Cisco EPN Manager Server.

Step 2 Install the geo map files on the primary server, as described in Install the Geo Map Resource Files on the Cisco EPN Manager Server .

Step 3 Install the geo map files on the secondary server, as described in Install the Geo Map Resource Files on the Cisco EPN Manager Server .

Step 4 On the primary server, enable the use of installed map files, as described in Configure the Cisco EPN Manager Server to Use the Installed Map Resources .

Step 5 On the primary server, check that the geo map is displayed, as described in Verify that the Geo Maps Files Were Installed Successfully.

Update Geo Map Resource Files After Upgrading to Cisco EPN Manager

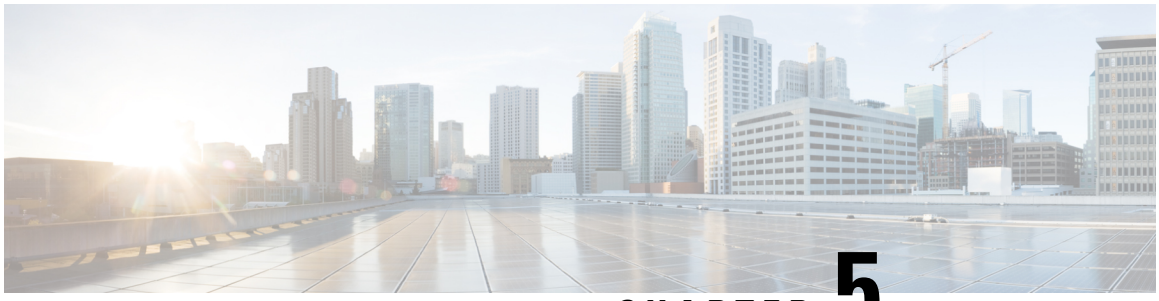
Geo map files must be reinstalled after upgrade.

Step 1 Download the required Cisco EPN Manager geo map files and reinstall them.

Step 2 Stop and restart the server(s).

Step 3 Clear the cache.

Step 4 Verify that the geo map files have been installed. See Verify that the Geo Maps Files Were Installed Successfully.

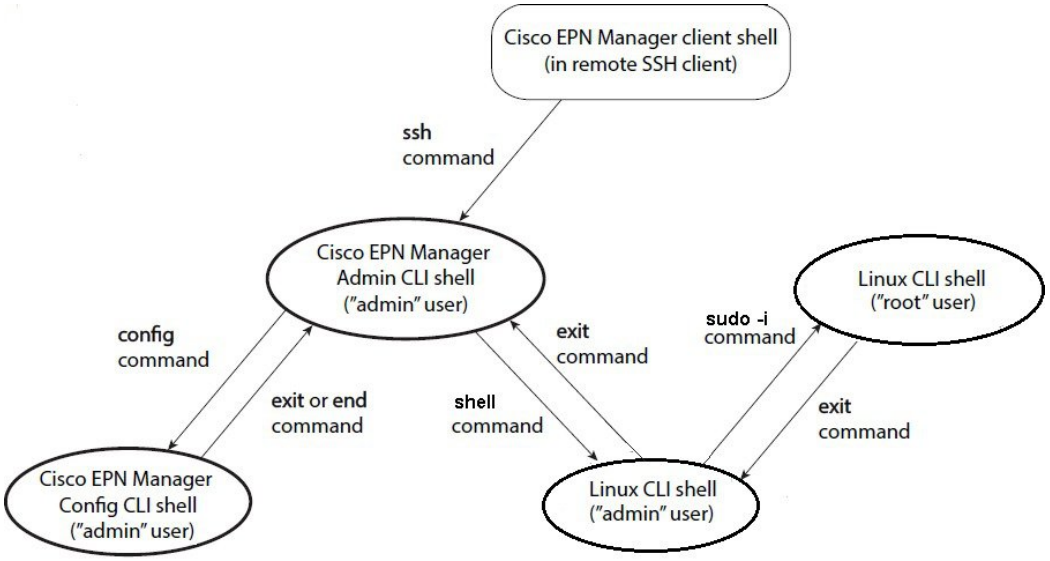


CHAPTER 5

Supplementary Installation-Related Information and Procedures

Log In and Out as the Linux CLI Users

The Linux CLI has two shell users: One with administrative access (Linux CLI admin user), and another with root access (Linux CLI root user). The following diagram illustrates the flow for logging in and out as the various CLI users.



To log in as the Linux CLI root user, you will have to transition from being the Cisco EPN Manager **CLI admin user** to the **Linux CLI root user**. The following procedure gives you the exact steps you must follow to log in as these users. For more information on these users, refer to the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Before You Begin

If the Linux CLI user is disabled, re-enable it. Refer to the user management procedures in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Step 1 To log in as the Linux CLI root user:

1. Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
2. As the Cisco EPN Manager CLI admin user, log in as the Linux CLI admin user:

```
shell
Enter shell access password:
password
```

3. Log in as the Linux CLI root user:

```
sudo -i
```

By default, the Linux CLI shell prompt is the same for the Linux CLI admin and root user. You can use the **whoami** command to check the current user.

Step 2 To exit:

1. Log out as the Linux CLI root user.

```
exit
```

You are now logged in as the Linux CLI admin user.

2. Log out as the Linux CLI admin user:

```
exit
```

You are now logged in as the Cisco EPN Manager CLI admin user.

What to do next

For security purposes, disable the Linux CLI users. Refer to the user management procedures in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Copy Files From a Client Machine to the Cisco EPN Manager Server

Before You Begin

You can use SCP, FTP, or SFTP protocols to retrieve files from the client machine. Make sure the required protocol is enabled on your client machine and the required ports are open (see Ports Used by Cisco EPN Manager).

This procedure explains how to copy files from your client machine to the Cisco EPN Manager server.

Step 1 Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.

Step 2 Log in as the Linux CLI admin user (see Log In and Out as the Linux CLI Users).

Step 3 From the Cisco EPN Manager server, retrieve the file from the client machine. You can use SCP, FTP, or SFTP. This example uses the **scp** command, which has the following syntax:

```
scpclientUsername@clientIP:/fullpath-to-file-on-client
/server-directory
```

Where:

- *clientUsername* is your username on the client machine
- *clientIP* is the IP address of the client machine
- *fullpath-to-file-on-client* is the full path to the file on the client machine that you want to copy to the server
- *server-directory* is the path to the directory on the server to which you want to copy the file

In the following example, a file named **myfile** located in the /temp directory on the client machine is being copied to the /localdisk/defaultRepo on the Cisco EPN Manager server.

```
scp joesmith@123.456.789.101:/temp/myfile /localdisk/defaultRepo
```

Step 4 Log out as the Linux CLI admin user as described in Log In and Out as the Linux CLI Users.

Synchronize the Hardware and NTP Clock

This procedure synchronizes the hardware clock with the NTP clock using the **hwclock** command.

Step 1 Log in as the Linux CLI root user as described in Log In and Out as the Linux CLI Users.

Step 2 Check the NTP service status and ensure that NTP has obtained a stable time reference using the following commands. The following includes examples of the output you should see.

1. Ensure that ntpd is running.

```
service ntpd status
 ntpd (pid 3290) is running...
```

2. If ntpd (pid 3290) is not running, start it using the following command:

```
service ntpd start
```

(Repeat *Step a* to ensure it is running.)

3. Ensure that NTP is receiving time from an NTP server.

```
ntpstat
 synchronised to NTP server (10.116.133.175) at stratum 3    time correct to within 62 ms
polling server every 1024 s
```

If you do not see output similar to this, then NTP synchronization has not yet occurred. Wait a few minutes and run **ntpstat** again. If synchronization does not happen within 10 minutes, contact your system administrator or Cisco support.

Step 3 Synchronize the hardware clock with NTP using the following command:

```
hwclock --systohc --debug
```

You should see output similar to the following:

```
hwclock from util-linux-ng 2.17.2
Using /dev interface to clock.
Last drift adjustment done at 1470117750 seconds after 1969
Last calibration done at 1470117750 seconds after 1969
Hardware clock is on local time
Assuming hardware clock is kept in local time.
Waiting for clock tick...
...got clock tick
Time read from Hardware Clock: 2016/08/02 16:03:30
Hw clock time : 2016/08/02 16:03:30 = 1470117810 seconds since 1969
1470117810.500000 is close enough to 1470117810.500000 (0.000000 < 0.001000)
Set RTC to 1470117810 (1470117810 + 0; refsystime = 1470117810.000000)
Setting Hardware Clock to 16:03:30 = 1470117810 seconds since 1969
ioctl(RTC_SET_TIME) was successful.
Not adjusting drift factor because it has been less than a day since the last calibration.
root$
```

Step 4 Verify that the hardware clock is synchronized with NTP.

```
echo "hwclock is: $(hwclock --show)" ; echo "linux clock is: $(date)";
```

Check the output and ensure that the two clocks are synchronized (to at least within a few seconds of each other):

```
Hwclock is: Tue 26 Jul 2016  06:11:40  PM AEST   -0.391028 secondslinux clock is: Tue Jul 26  18:11:40
  AEST 2016
```

Step 5 As the Linux CLI admin user, restart the Cisco EPN Manager services.

- If you are logged in as the Linux CLI root user, switch to the Linux CLI admin user.

  ```
  exit
  ```

- Switch to the Cisco EPN Manager CLI admin user.

  ```
  exit
  ```

- Stop and restart the Cisco EPN Manager services.

  ```
  ncs stop
  ncs start
  ```

Log Into the Cisco EPN Manager Web GUI

Follow these steps to log into the Cisco EPN Manager web GUI:

Procedure

Step 1 On a client machine, launch one of the supported browsers (see Web Client Requirements).

Step 2 In the browser's address line, enter **`https://serverIP`**, where *serverIP* is the IP address of the server on which you installed Cisco EPN Manager. The login window is displayed.

When a client accesses the Cisco EPN Manager web GUI for the first time, the browser may display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Cisco EPN Manager server. After you complete this procedure, the browser will accept the Cisco EPN Manager server as a trusted site in all future login attempts.

Step 3 Enter the web GUI root username and password, as specified during the installation.

If any licensing problems occur, a message appears in an alert box. If you have an evaluation license, the number of days until the license expires is shown. You are also alerted about any expired licenses. (You have the option to go directly to the **Administration** > **Licenses and Software Updates** > **Licenses** page to address these problems.) For more information about licenses, refer to the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Step 4 Click **Login** to log in to the Cisco EPN Manager web GUI. The home page appears and you can now use the web GUI. For information about the dashboards and dashlets, refer to the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Step 5 For increased security, perform these steps:

1. Change the password for the web GUI root user by choosing **Administration** > **Users** > **Roles & AAA** > **Change Password**.
2. Create at least one Cisco EPN Manager web GUI user that has Admin or Super User privileges, then disable the web GUI root user. For information on disabling this user, refer to the user management topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide .
3. If you have not done so already, disable the Linux CLI users. Refer to the Cisco Evolved Programmable Network Manager User and Administrator Guide .

What to do next

Perform setup tasks for server, user, fault, and web GUI management. For a detailed list of tasks, see the beginning of the administration section of the Cisco Evolved Programmable Network Manager User and Administrator Guide .

For information on Cisco EPN Manager user interfaces and user types, Cisco Evolved Programmable Network Manager User and Administrator Guide .

Time Zones Supported by Cisco Evolved Programmable Network Manager

This table lists the available values for the system time zone.

Africa/Abidjan	America/St_Johns	Etc/GMT+6
Africa/Accra	America/St_Kitts	Etc/GMT+7
Africa/Addis_Ababa	America/St_Lucia	Etc/GMT+8
Africa/Algiers	America/St_Thomas	Etc/GMT+9
Africa/Asmara	America/St_Vincent	Etc/GMT0
Africa/Asmera	America/Swift_Current	Etc/GMT-0
Africa/Bamako	America/Tegucigalpa	Etc/GMT-1
Africa/Bangui	America/Thule	Etc/GMT-10
Africa/Banjul	America/Thunder_Bay	Etc/GMT-11
Africa/Bissau	America/Tijuana	Etc/GMT-12
Africa/Blantyre	America/Toronto	Etc/GMT-13
Africa/Brazzaville	America/Tortola	Etc/GMT-14
Africa/Bujumbura	America/Vancouver	Etc/GMT-2
Africa/Cairo	America/Virgin	Etc/GMT-3
Africa/Casablanca	America/Whitehorse	Etc/GMT-4
Africa/Ceuta	America/Winnipeg	Etc/GMT-5
Africa/Conakry	America/Yakutat	Etc/GMT-6
Africa/Dakar	America/Yellowknife	Etc/GMT-7
Africa/Dar_es_Salaam	Antarctica/Casey	Etc/GMT-8
Africa/Djibouti	Antarctica/Davis	Etc/GMT-9
Africa/Douala	Antarctica/DumontDUrville	Etc/Greenwich
Africa/El_Aaiun	Antarctica/Mawson	Etc/UCT
Africa/Freetown	Antarctica/McMurdo	Etc/Universal
Africa/Gaborone	Antarctica/Palmer	Etc/UTC
Africa/Harare	Antarctica/Rothera	Etc/Zulu

Africa/Johannesburg	Antarctica/South_Pole	Europe/Amsterdam
Africa/Kampala	Antarctica/Syowa	Europe/Andorra
Africa/Khartoum	Antarctica/Vostok	Europe/Athens
Africa/Kigali	Arctic/Longyearbyen	Europe/Belfast
Africa/Kinshasa	Asia/Aden	Europe/Belgrade
Africa/Lagos	Asia/Almaty	Europe/Berlin
Africa/Libreville	Asia/Amman	Europe/Bratislava
Africa/Lome	Asia/Anadyr	Europe/Brussels
Africa/Luanda	Asia/Aqtau	Europe/Bucharest
Africa/Lubumbashi	Asia/Aqtobe	Europe/Budapest
Africa/Lusaka	Asia/Ashgabat	Europe/Chisinau
Africa/Malabo	Asia/Ashkhabad	Europe/Copenhagen
Africa/Maputo	Asia/Baghdad	Europe/Dublin
Africa/Maseru	Asia/Bahrain	Europe/Gibraltar
Africa/Mbabane	Asia/Baku	Europe/Guernsey
Africa/Mogadishu	Asia/Bangkok	Europe/Helsinki
Africa/Monrovia	Asia/Beirut	Europe/Isle_of_Man
Africa/Nairobi	Asia/Bishkek	Europe/Istanbul
Africa/Ndjamena	Asia/Brunei	Europe/Jersey
Africa/Niamey	Asia/Calcutta	Europe/Kaliningrad
Africa/Nouakchott	Asia/Choibalsan	Europe/Kiev
Africa/Ouagadougou	Asia/Chongqing	Europe/Lisbon
Africa/Porto-Novo	Asia/Chungking	Europe/Ljubljana
Africa/Sao_Tome	Asia/Colombo	Europe/London
Africa/Timbuktu	Asia/Dacca	Europe/Luxembourg
Africa/Tripoli	Asia/Damascus	Europe/Madrid
Africa/Tunis	Asia/Dhaka	Europe/Malta
Africa/Windhoek	Asia/Dili	Europe/Mariehamn
America/Adak	Asia/Dubai	Europe/Minsk

America/Anchorage	Asia/Dushanbe	Europe/Monaco
America/Anguilla	Asia/Gaza	Europe/Moscow
America/Antigua	Asia/Harbin	Europe/Nicosia
America/Araguaina	Asia/Ho_Chi_Minh	Europe/Oslo
America/Argentina/	Asia/Hong_Kong	Europe/Paris
America/Argentina/	Asia/Hovd	Europe/Podgorica
America/Argentina/Catamarca	Asia/Irkutsk	Europe/Prague
America/Argentina/Cordoba	Asia/Istanbul	Europe/Riga
America/Argentina/Jujuy	Asia/Jakarta	Europe/Rome
America/Argentina/La_Rioja	Asia/Jayapura	Europe/Samara
America/Argentina/Mendoza	Asia/Jerusalem	Europe/San_Marino
America/Argentina/Rio_Gallegos	Asia/Kabul	Europe/Sarajevo
America/Argentina/Salta	Asia/Kamchatka	Europe/Simferopol
America/Argentina/San_Juan	Asia/Karachi	Europe/Skopje
America/Argentina/San_Luis	Asia/Kashgar	Europe/Sofia
America/Argentina/Tucuman	Asia/Kathmandu	Europe/Stockholm
America/Argentina/Ushuaia	Asia/Katmandu	Europe/Tallinn
America/Aruba	Asia/Kolkata	Europe/Tirane
America/Asuncion	Asia/Krasnoyarsk	Europe/Tiraspol
America/Atikokan	Asia/Kuala_Lumpur	Europe/Uzhgorod
America/Atka	Asia/Kuching	Europe/Vaduz
America/Bahia	Asia/Kuwait	Europe/Vatican
America/Barbados	Asia/Macao	Europe/Vienna
America/Belem	Asia/Macau	Europe/Vilnius
America/Belize	Asia/Magadan	Europe/Volgograd
America/Blanc-Sablon	Asia/Makassar	Europe/Warsaw
America/Boa_Vista	Asia/Manila	Europe/Zagreb
America/Bogota	Asia/Muscat	Europe/Zaporozhye
America/Boise	Asia/Nicosia	Europe/Zurich

America/Buenos_Aires	Asia/Novosibirsk	Factory
America/Cambridge_Bay	Asia/Omsk	GB
America/Campo_Grande	Asia/Oral	GB-Eire
America/Cancun	Asia/Phnom_Penh	GMT
America/Caracas	Asia/Pontianak	GMT+0
America/Catamarca	Asia/Pyongyang	GMT0
America/Cayenne	Asia/Qatar	GMT-0
America/Cayman	Asia/Qyzylorda	Greenwich
America/Chicago	Asia/Rangoon	Hongkong
America/Chihuahua	Asia/Riyadh	HST
America/Coral_Harbour	Asia/Riyadh87	Iceland
America/Cordoba	Asia/Riyadh88	Indian/Antananarivo
America/Costa_Rica	Asia/Riyadh89	Indian/Chagos
America/Cuiaba	Asia/Saigon	Indian/Christmas
America/Curacao	Asia/Sakhalin	Indian/Cocos
America/Danmarkshavn	Asia/Samarkand	Indian/Comoro
America/Dawson	Asia/Seoul	Indian/Kerguelen
America/Dawson_Creek	Asia/Shanghai	Indian/Mahe
America/Denver	Asia/Singapore	Indian/Maldives
America/Detroit	Asia/Taipei	Indian/Mauritius
America/Dominica	Asia/Tashkent	Indian/Mayotte
America/Edmonton	Asia/Tbilisi	Indian/Reunion
America/Eirunepe	Asia/Tehran	Iran
America/El_Salvador	Asia/Tel_Aviv	Israel
America/Ensenada	Asia/Thimbu	Jamaica
America/Fort_Wayne	Asia/Thimphu	Japan
America/Fortaleza	Asia/Tokyo	Kwajalein
America/Glace_Bay	Asia/Ujung_Pandang	Libya
America/Godthab	Asia/Ulaanbaatar	MET

America/Goose_Bay	Asia/Ulan_Bator	Mexico/BajaNorte
America/Grand_Turk	Asia/Urumqi	Mexico/BajaSur
America/Grenada	Asia/Vientiane	Mexico/General
America/Guadeloupe	Asia/Vladivostok	Mideast/Riyadh87
America/Guatemala	Asia/Yakutsk	Mideast/Riyadh88
America/Guayaquil	Asia/Yekaterinburg	Mideast/Riyadh89
America/Guyana	Asia/Yerevan	MST
America/Halifax	Atlantic/Azores	MST7MDT
America/Havana	Atlantic/Bermuda	Navajo
America/Hermosillo	Atlantic/Canary	New_Salem
America/Indiana/Indianapolis	Atlantic/Cape_Verde	NZ
America/Indiana/Knox	Atlantic/Faeroe	NZ-CHAT
America/Indiana/Marengo	Atlantic/Faroe	Pacific/Apia
America/Indiana/Petersburg	Atlantic/Jan_Mayen	Pacific/Auckland
America/Indiana/Tell_City	Atlantic/Madeira	Pacific/Chatham
America/Indiana/Vevay	Atlantic/Reykjavik	Pacific/Easter
America/Indiana/Vincennes	Atlantic/South_Georgia	Pacific/Efate
America/Indiana/Winamac	Atlantic/St_Helena	Pacific/Enderbury
America/Indianapolis	Atlantic/Stanley	Pacific/Fakaofo
America/Inuvik	Australia/ACT	Pacific/Fiji
America/Iqaluit	Australia/Adelaide	Pacific/Funafuti
America/Jamaica	Australia/Brisbane	Pacific/Galapagos
America/Jujuy	Australia/Broken_Hill	Pacific/Gambier
America/Juneau	Australia/Canberra	Pacific/Guadalcanal
America/Kentucky/Louisville	Australia/Currie	Pacific/Guam
America/Kentucky/Monticello	Australia/Darwin	Pacific/Honolulu
America/Knox_IN	Australia/Eucla	Pacific/Johnston
America/La_Paz	Australia/Hobart	Pacific/Kiritimati
America/Lima	Australia/LHI	Pacific/Kosrae

America/Los_Angeles	Australia/Lindeman	Pacific/Kwajalein
America/Louisville	Australia/Lord_Howe	Pacific/Majuro
America/Maceio	Australia/Melbourne	Pacific/Marquesas
America/Managua	Australia/North	Pacific/Midway
America/Manaus	Australia/NSW	Pacific/Nauru
America/Marigot	Australia/Perth	Pacific/Niue
America/Martinique	Australia/Queensland	Pacific/Norfolk
America/Mazatlan	Australia/South	Pacific/Noumea
America/Mendoza	Australia/Sydney	Pacific/Pago_Pago
America/Menominee	Australia/Tasmania	Pacific/Palau
America/Merida	Australia/Victoria	Pacific/Pitcairn
America/Mexico_City	Australia/West	Pacific/Ponape
America/Miquelon	Australia/Yancowinna	Pacific/Port_Moresby
America/Moncton	Brazil/Acre	Pacific/Rarotong
America/Monterrey	Brazil/DeNoronha	Pacific/Saipan
America/Montevideo	Brazil/East	Pacific/Samoa
America/Montreal	Brazil/West	Pacific/Tahiti
America/Montserrat	Buenos_Aires	Pacific/Tarawa
America/Nassau	Canada/Atlantic	Pacific/Tongatapu
America/New_York	Canada/Central	Pacific/Truk
America/Nipigon	Canada/Eastern	Pacific/Wake
America/Nome	Canada/East-Saskatchewan	Pacific/Wallis
America/Noronha	Canada/Mountain	Pacific/Yap
America/North_Dakota/	Canada/Newfoundland	Poland
America/North_Dakota/Center	Canada/Pacific	Portugal
America/Panama	Canada/Saskatchewan	PRC
America/Pangnirtung	Canada/Yukon	PST8PDT
America/Paramaribo	CET	ROC
America/Phoenix	Chile/Continental	ROK

America/Port_of_Spain	Chile/EasterIsland	Singapore
America/Port-au-Prince	ComodRivadavia	Turkey
America/Porto_Acre	CST6CDT	UCT
America/Porto_Velho	Cuba	Universal
America/Puerto_Rico	EET	US/Alaska
America/Rainy_River	Egypt	US/Aleutian
America/Rankin_Inlet	Eire	US/Arizona
America/Recife	EST	US/Central
America/Regina	EST5EDT	US/Eastern
America/Resolute	Etc/GMT	US/East-Indiana
America/Rio_Branco	Etc/GMT+0	US/Hawaii
America/Rosario	Etc/GMT+1	US/Indiana-Starke
America/Santarem	Etc/GMT+10	US/Michigan
America/Santiago	Etc/GMT+11	US/Mountain
America/Santo_Domingo	Etc/GMT+12	US/Pacific
America/Sao_Paulo	Etc/GMT+2	US/Samoa
America/Scoresbysund	Etc/GMT+3	UTC
America/Shiprock	Etc/GMT+4	WET
America/St_Barthelemy	Etc/GMT+5	W-SU
		Zulu