



Cisco Evolved Programmable Network Manager 2.0

Installation Guide

First Published: May 2, 2016

Last Modified: November 8, 2016

- 1** [Installation Overview](#)
- 2** [System Requirements](#)
- 3** [Prepare for Installation](#)
- 4** [Install Cisco EPN Manager 2.0](#)
- 5** [Upgrade from an Earlier Version of Cisco EPN Manager](#)
- 6** [High Availability](#)
- 7** [Get Started with Cisco EPN Manager](#)
- 8** [Uninstall Cisco EPN Manager](#)
- 9** [Related Documentation](#)
- 10** [Obtaining Documentation and Submitting a Service Request](#)

1 Installation Overview

- [Installation Options](#)
- [Upgrade Options](#)
- [High Availability Overview](#)
- [Log In and Out as the Linux CLI Users](#)

Installation Options

You can install Cisco EPN Manager 2.0 either on a virtual machine (VM) or bare metal server:

- OVA/VM installation—For a VM installation, install the provided 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 provided 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.

For information on the advantages and disadvantages of each of these installation types, contact your Cisco representative.

Upgrade Options

If you are upgrading from previous releases of Cisco EPN Manager, you can use either of the following methods:



Note Cisco EPN Manager does not support rolling back to the previous version after an upgrade.

- Automatic Upgrade—This upgrade option is normally 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. This type of upgrade can cause a downtime, but after the upgrade, you do not have to restore your data from a backup. For more information, see Automatic Upgrade on page 28.
- Backup-Restore Upgrade—This upgrade option generally requires new hardware (although it is possible to use existing hardware). There is no downtime in this type of upgrade. Your 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.

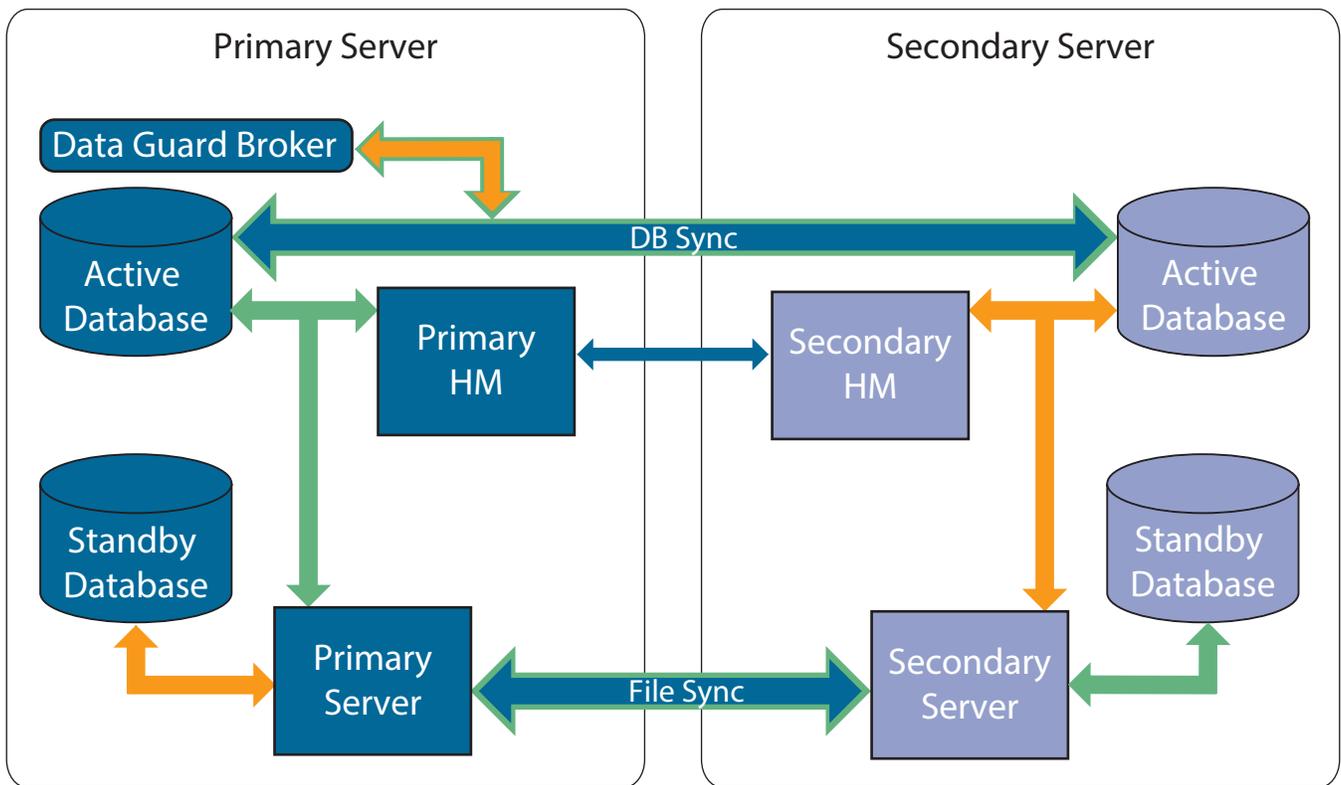
To use either of these upgrade options, your deployment must be running Cisco EPN Manager 1.2.7 (that is, Cisco EPN Manager 1.2 with Maintenance Pack 7). For information on how to install Cisco EPN Manager 1.2.7, see the [release notes](#) for that maintenance pack.

High Availability Overview

The Cisco EPN Manager high availability (HA) framework 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. Servers can fail due to issues in one or more of the following areas:

- Application processes—Server, TFTP, FTP, and other process failures.
- Database server—Database-related process failures (the database server runs as a service on Cisco EPN Manager).
- Network—Problems with network access or reachability.
- System—Problems with the server's physical hardware or operating system.
- Virtual machine—Problems with the VM environment on which the primary and secondary servers are installed.

The following figure shows the main components and process flows for an HA setup.



An HA 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 (either automatically 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 failover.

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 a failback is triggered, the primary server again takes over the active role. This role switching between the primary and secondary servers happens within two to three minutes.

Synchronizations between the primary and secondary servers fall under two categories:

- File changes—File changes are synchronized using the HTTPS protocol and include changes in report configurations, configuration templates, TFTP-root directory, administration settings, licensing files, the key store, and so forth. File synchronization is done in:
 - Batches—For files that are not updated frequently, such as license files. These files are synchronized once every 500 seconds.
 - Near real-time—For files that are updated frequently. These files are synchronized once every 11 seconds.
- Database changes—These changes are related to configuration, performance, and monitoring data. These are synchronized using Oracle Recovery Manager (RMAN), which creates the initial standby database, and Oracle Active Data Guard, which synchronizes the databases when a change occurs.

As part of the synchronization process, the primary and secondary servers exchange the following messages:

- Database Sync messages—Includes all the information necessary to ensure that the databases on the primary and secondary servers are running and synchronized.
- File Sync messages—Includes frequently-updated configuration files. These are synchronized in batches or near real-time, as explained previously.
- Process Sync messages—Includes information about whether the application- and database-related processes are running. These messages fall under the Heartbeat category.
- Health Monitor Sync messages—Includes information about reports, network, system, and Health Monitor failure conditions.

Standard HA installations have one distinct IP address/URL for the primary server and a second IP address/URL for the secondary server. In these deployments, you must configure your devices to forward events to both the primary and secondary server. Alternatively, for local HA deployment models, you can set up HA so that it uses a virtual IP address, which is a single IP address/URL that is always associated with the active server (primary or secondary). In this case, you only need to configure your devices to forward events to the single IP address/URL. For more information, see [High Availability](#).

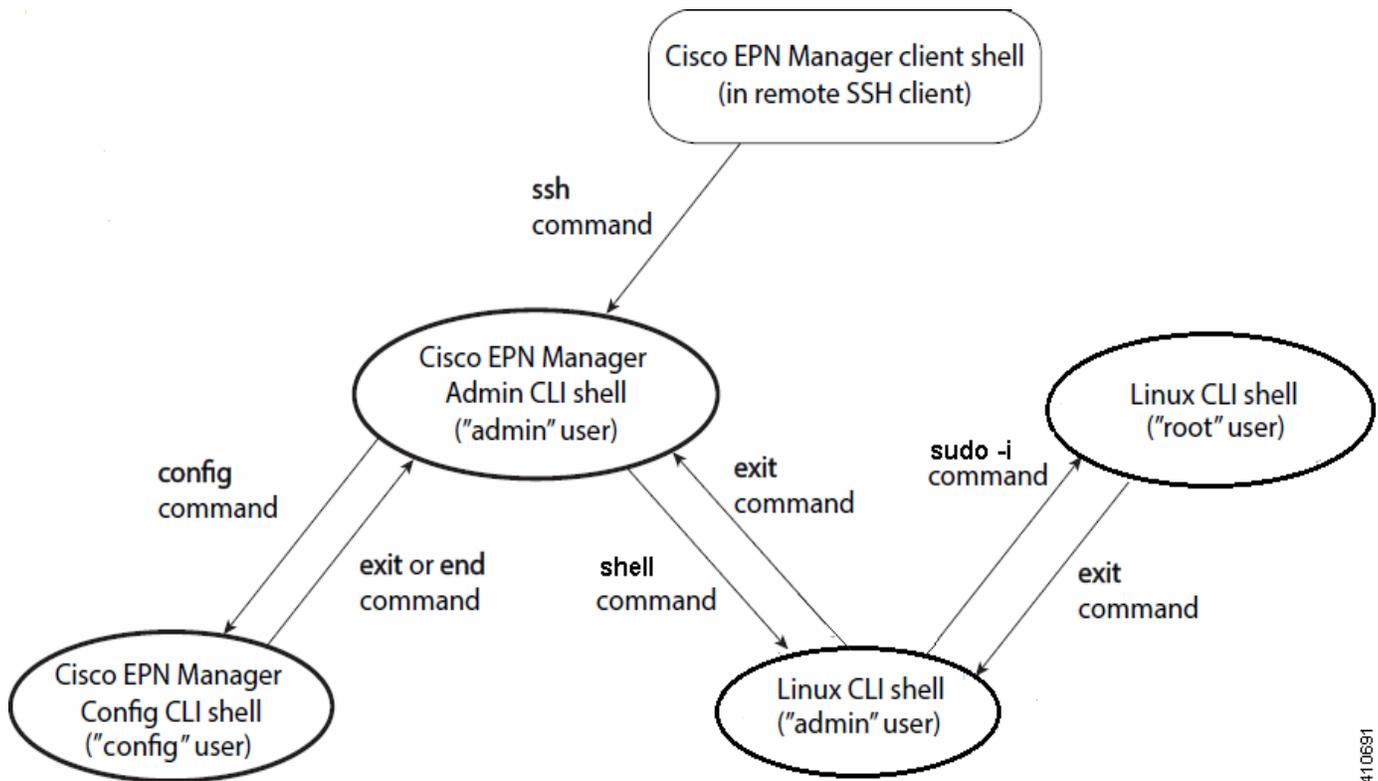
Whether your HA deployment uses a single IP address or not, users should always connect to the Cisco EPN Manager web GUI using the active server IP address/URL.

Log In and Out as the Linux CLI Users

In different parts of the installation process, you will have to log in as a Linux CLI. The login process is different between Cisco EPN Manager 2.x and Cisco EPN Manager 1.2.x. The Cisco EPN Manager 1.2.x procedures are included for deployments that plan to perform an upgrade.

How to Log In and Out as the Linux CLI User in Cisco EPN Manager 2.x: Complete Workflow

In Cisco EPN Manager 2.x, 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 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](#).

410691

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](#).

Procedure

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

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

```
shell
```

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

- c. 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 **whomai** command to check the current user.

Step 2 To exit:

- a. Log out as the Linux CLI root user.

```
exit
```

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

- b. Log out as the Linux CLI admin user:

```
exit
```

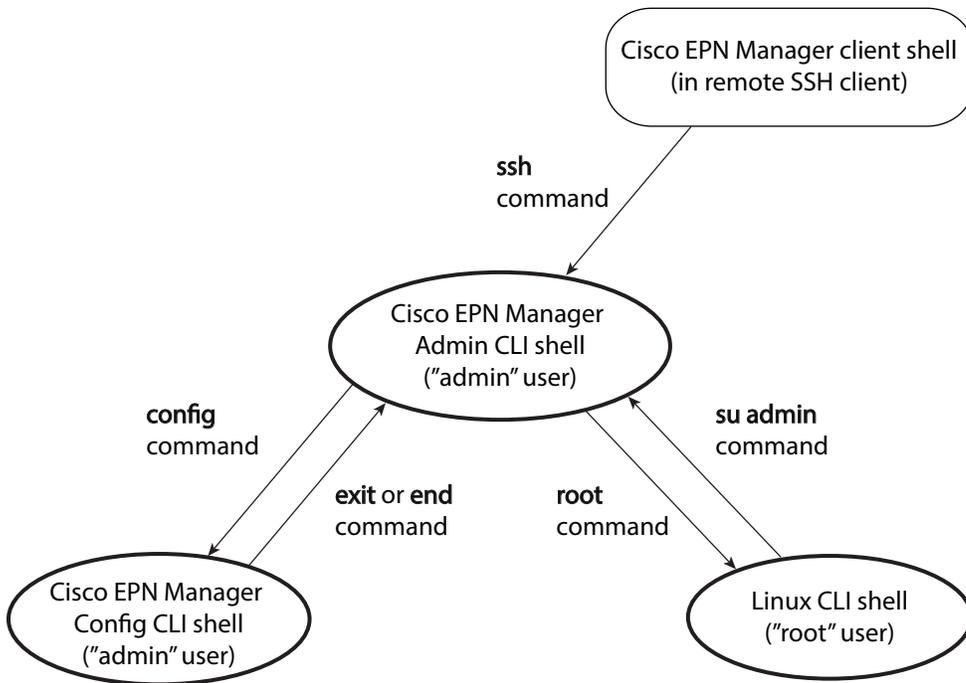
You are now logged in as the Cisco EPN Manager CLI admin user.

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](#).

How to Log In and Out as the Linux CLI User in Cisco EPN Manager 1.2.x: Complete Workflow

In Cisco EPN Manager 1.2.x, the Linux CLI has one shell user that has root access (Linux CLI root user). The following diagram illustrates the flow for logging in and out as the various CLI users.



402398

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. 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](#).

Procedure

-
- Step 1** To log in as the Linux CLI root user:
- a. Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
 - b. As the Cisco EPN Manager CLI admin user, log in as the Linux CLI root user:


```

root
Enter shell access password: password

```

- Step 2** To exit, log out as the Linux CLI root user:
- ```

su admin

```

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

---

### What To Do Next

For security purposes, disable the Linux CLI root user. Refer to the user management procedures in the [Cisco Evolved Programmable Network Manager User and Administrator Guide](#).

## 2 System Requirements

- [Hardware and Software Requirements](#)
- [Web Client Requirements](#)
- [Scale Requirements \(Professional Installation Option\)](#)
- [Ports Used by Cisco EPN Manager](#)

### Hardware and Software Requirements

- [Operating System Requirements](#)
- [OVA/VM Requirements](#)
- [Bare Metal Requirements](#)

### Operating System Requirements

The following table summarizes the operating system requirements for Cisco EPN Manager.

| Cisco EPN Manager Version | Red-Hat Enterprise Linux (RHEL) Version | Oracle Database Version <sup>1</sup>                                          |
|---------------------------|-----------------------------------------|-------------------------------------------------------------------------------|
| Cisco EPN Manager 1.2.0   | RHEL 5.11                               | Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 (64-bit production) |
| Cisco EPN Manager 2.0.0   | RHEL 6.7                                | Oracle Database 12c Enterprise Edition Release 12.1.0.2 (64-bit production)   |

1. The Oracle software is embedded in the Cisco EPN Manager software.

### OVA/VM Requirements

The following table summarizes the OVA/VM system requirements for the Standard and Professional system size options. (Although Express and Express Plus system size options are also available, they should only be used for demo and lab purposes.)



**Note** Due to the increase in services that are supported by Cisco EPN Manager, we recommend that you use the Professional system size option for both OVA/VM and ISO/bare metal installations.

| Item            |                                  | Standard   | Professional |
|-----------------|----------------------------------|------------|--------------|
| Virtual Machine | VMware ESXi version <sup>1</sup> | 5.1 or 5.5 | 5.1 or 5.5   |
|                 | 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                   | 450 MBps   | 450 MBps     |

1. 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.

## Bare Metal Requirements

The following table summarizes the OVA/VM system requirements for the Standard and Professional system size options. (Although Express and Express Plus system size options are also available, they should only be used for demo and lab purposes.)



**Note** Due to the increase in services that are supported by Cisco EPN Manager, we recommend that you use the Professional system size option for both OVA/VM and ISO/bare metal installations.

For bare metal installations, Cisco EPN Manager can only be installed on the Cisco UCS server (Gen 2) as a rack-mounted server with the following requirements.

### Bare Metal Requirements for Standard Deployments (No High Availability)

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

| Item       |                        | Standard          | Professional      |
|------------|------------------------|-------------------|-------------------|
| Bare metal | Appliance image format | ISO               | ISO               |
|            | Equivalent 1.x option  | Physical server   | Physical server   |
| Hardware   | CPU (cores/threads)    | 1xCPU (10 C/20 T) | 1xCPU (10 C/20 T) |
|            | Memory                 | 48 GB             | 64 GB             |
|            | Disk capacity          | 4x300 GB          | 4x900 GB          |
|            | Disk I/O speed         | 450 MBps          | 450 MBps          |
|            | RAID Level             | RAID 10           | 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 [High Availability](#).

| Hardware                                  | Requirement                                        |
|-------------------------------------------|----------------------------------------------------|
| Cisco UCS server type                     | Cisco UCS C220 M4S (as a rack-mounted server)      |
| 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)       |
| Memory                                    | 64 GB                                              |
| RAID level                                | RAID 10                                            |
| Number of NICs                            | 1                                                  |
| Disk capacity                             | 4x900 GB                                           |
| Virtual hard disk size in RAID controller | 1 TB                                               |
| 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 latency   | Maximum: 10 milliseconds or less             |
| Network bandwidth | Ideal: 977 Mbps<br>Minimum: 255 Mbps or more |

## Web Client Requirements

Cisco EPN Manager users access the product using a web browser client. The following lists the client and browser requirements.

- Hardware—Mac or Windows laptop or desktop compatible with one of the tested and supported browsers listed next
- Browsers
  - Google Chrome 45 or later
  - Mozilla Firefox ESR 38
  - Mozilla Firefox 39 or later
  - Microsoft Internet Explorer 11.0
- Recommended display resolution—1600x900 pixels or higher (minimum: 1366x768)

## Scale Requirements (Professional Installation Option)

The following table summarizes the maximum level of support for a system size deployment in both OVA/VM and ISO/bare metal installations.



**Note** Support for WiFi access points and WiFi controllers has been deprecated. For more information about deprecated support for device families, refer to the [release notes](#) for the Cisco EPN Manager 2.0 maintenance packs.

These scale numbers are for a Cisco EPN Manager Professional deployment that uses the default system settings.

| 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                                                    | 300     |
|                 | 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   |
| Monitoring      | Sustained rate of events (events/sec)                                                                  | 100     |
|                 | Maximum interfaces per device                                                                          | 2,100   |
| 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? | Procedure to Disable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------|----------|-------------------------------------------------------------------------------------------------------------------------------------|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 21   | TCP      | To transfer files to and from devices using FTP.                                                                                    | Yes              | To disable FTP:<br><ol style="list-style-type: none"><li>1. From the web GUI, choose <b>Administration &gt; Settings &gt; System Settings</b>, then choose <b>General &gt; Server</b>.</li><li>2. Under <b>FTP</b>, choose <b>Disable</b>.</li><li>3. As the Cisco EPN Manager CLI admin user, stop and restart the server to apply your changes:<br/><pre>ncs stop ncs start</pre></li></ol> To re-enable FTP:<br><ol style="list-style-type: none"><li>1. From the web GUI, choose <b>Administration &gt; Settings &gt; System Settings</b>, then choose <b>General &gt; Server</b>.</li><li>2. Under <b>FTP</b>, choose <b>Enable</b>.</li><li>3. As the Cisco EPN Manager CLI admin user, stop and restart the server to apply your changes:<br/><pre>ncs stop ncs start</pre></li></ol> |
| 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 supports 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 is used for image distribution, and if supported by the managed devices.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

**Table 1** *Listening Ports That Are Open Through Built-in Firewall (continued)*

| Port | Protocol | Usage                                                                                                                                                                               | Safe to Disable?      | Procedure to Disable                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 80   | TCP      | PnP (via HTTP protocol).                                                                                                                                                            | Yes                   | <p>Cisco EPN Manager does not support the PnP feature. You should disable this traffic in the network firewall.</p> <p>To disable:</p> <ol style="list-style-type: none"> <li>1. From the web GUI, choose <b>Administration &gt; Settings &gt; System Settings</b>, then choose <b>General &gt; Server</b>.</li> <li>2. Under <b>HTTP Forward</b>, choose <b>Disable</b>.</li> <li>3. As the Cisco EPN Manager CLI admin user, enter the following commands to apply the settings and shut down the PnP gateway (enter the commands in this sequence):</li> </ol> <pre> <b>ncs pnp-gateway disable</b> <b>ncs stop</b> <b>ncs start</b> </pre> |
| 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      | <p>For High Availability (HA) communication between active and standby Cisco EPN Manager servers.</p> <p>Used to allow Oracle JDBC traffic for Oracle database synchronization.</p> | Yes                   | If at least one Cisco EPN Manager server is not configured for HA, this port is automatically disabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 2021 | TCP      | To distribute images to devices using FTP.                                                                                                                                          | No                    | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 8082 | TCP      | <p>For the HA Health Monitor web interface (via HTTP).</p> <p>Used by primary and secondary servers to monitor their health status via HTTP.</p>                                    | No (If HA configured) | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| 8087 | TCP      | To update software on the HA secondary backup server (uses HTTPS as transport).                                                                                                     | No                    | —                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

**Table 1** *Listening Ports That Are Open Through Built-in Firewall (continued)*

| Port           | Protocol | Usage                                                                                                        | Safe to Disable? | Procedure to Disable                                                                                                                                                                                                                                                                                                        |
|----------------|----------|--------------------------------------------------------------------------------------------------------------|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. To disable the PnP port enter the following commands in this sequence (you must be logged in as the Cisco EPN Manager CLI admin user):<br><br><pre> <b>ncs pnp-gateway disable</b> <b>ncs stop</b> <b>ncs start</b> </pre> |
| 61617          | TCP      | For MTOSI NBI notification over Java Message Service (JMS) connections.<br><br>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.

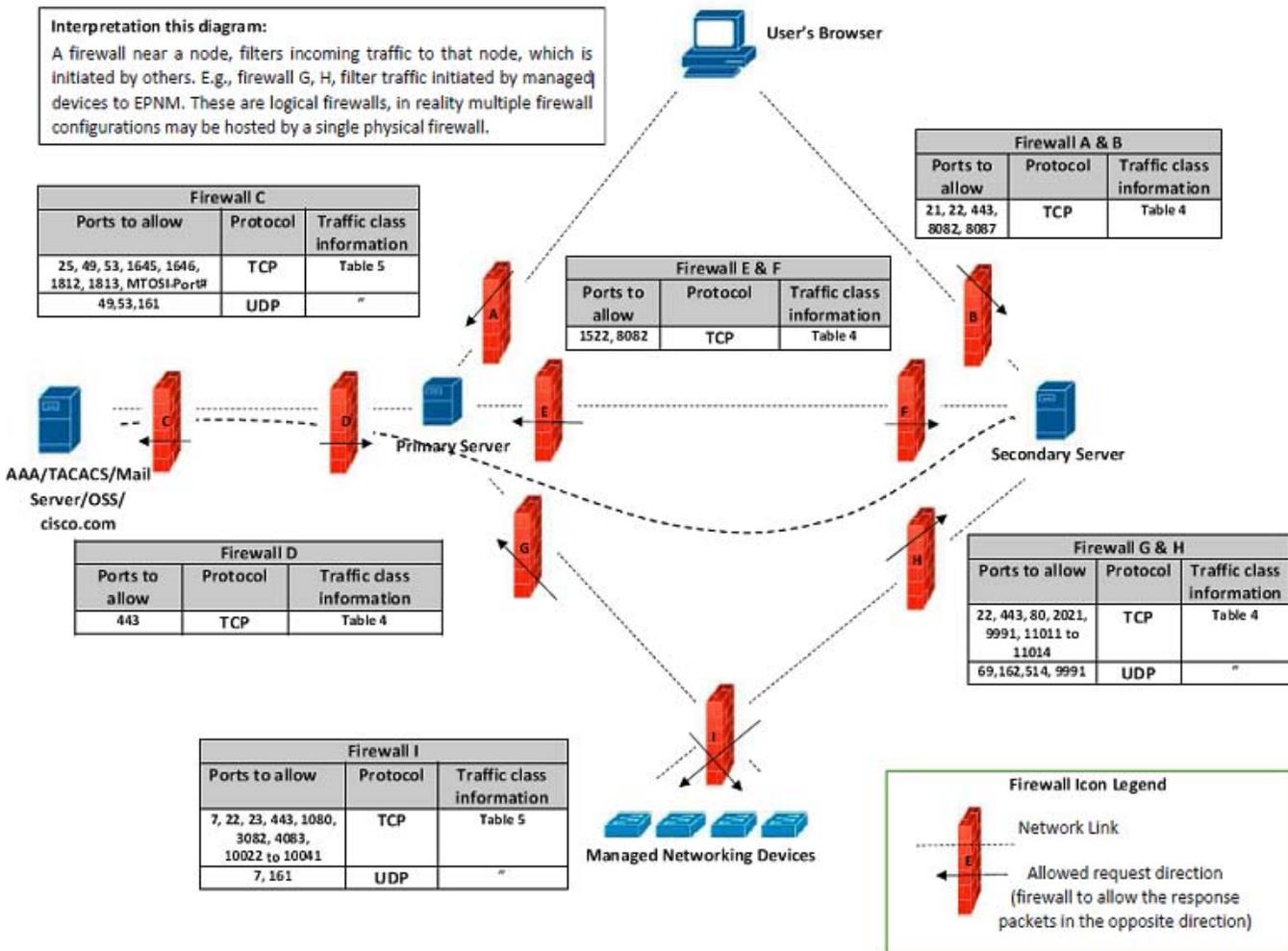
**Table 2** *Destination Ports Used by Cisco EPN Manager*

| Port                       | Protocol | Used to:                                                                                                                                                     |
|----------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7                          | TCP/UDP  | Discover endpoints using ICMP.                                                                                                                               |
| 22                         | TCP      | Initiate SSH connections with managed devices.                                                                                                               |
| 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 TL1 protocol.                                                                             |

**Table 2 Destination Ports Used by Cisco EPN Manager (continued)**

| Port                         | Protocol | Used to:                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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).                                                                                                                                                                                                                                                                     |
| <i>MTOSI TCP port number</i> | 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 <a href="#">Cisco Evolved Programmable Network Manager MTOSI API Guide for OSS Integration</a> 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 1. We recommend that you disable the ports that are used by services that are not supported in Cisco EPN Manager.



## 3 Prepare for Installation

- [Licensing](#)
- [Prerequisites for OVA/VM Installations](#)
- [Prerequisites for ISO/Bare Metal Installations](#)
- [Verify the ISO Image or OVA Package](#)

### Licensing

Make sure you have the necessary licenses for your installation. Licenses determine the features you can use (such as the NBI or High Availability) and the type and number of devices that Cisco EPN Manager can manage. To purchase new licenses, go to the [Product License Registration page](#). To install a new license, the original license must reside on the server. Do not create copies of licenses.

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](#).
- 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](#).
- The following software is installed:
  - Java with JRE Version 1.6.0.14
  - Flash Driver v9.0.246 or higher
- The downloaded ISO image has been verified as described in [Verify the ISO Image or OVA Package](#).

## 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.

### Procedure

---

**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 2.0 product OVA package or ISO image to be verified (\*.iso or \*.ova)
- The Cisco EPNM 2.0 OVA or ISO signature file (\*.signature)
- The Cisco EPNM 2.0 certificate file (\*.pem)

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

**Step 3** Move to the temporary directory and run the following command. You must run this command as the Linux CLI root user. (See [How to Log In and Out as the Linux CLI User in Cisco EPN Manager 1.2.x: Complete Workflow](#). Be sure to use the procedures for Cisco EPN Manager 1.2.x.)

```
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 4** If the result is **Verified OK**:

- For an OVA package, proceed to [Step 5](#).
- For an ISO file, go to [Install Cisco EPN Manager 2.0](#).



---

**Note** (ISO/bare metal automatic upgrades) If you are using this procedure to validate the `patching_upgrade.pl` script, return to [Step 7 of Perform an Automatic Upgrade \(High Availability\)](#) and run the script.

---

**Step 5** (OVA packages only) Verify the publisher and certificate chain using the VMware vSphere client.

a. Verify that Cisco Systems is the publisher:

- In the VMware vSphere client, choose **File > Deploy OVF Template**.
- Browse to the OVA installation file (\*.ova) and select it, then click **Next**.
- Check whether the Publisher field in the OVF Template Details window displays **Cisco Systems, Inc** with a green check mark next to it.



---

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

---

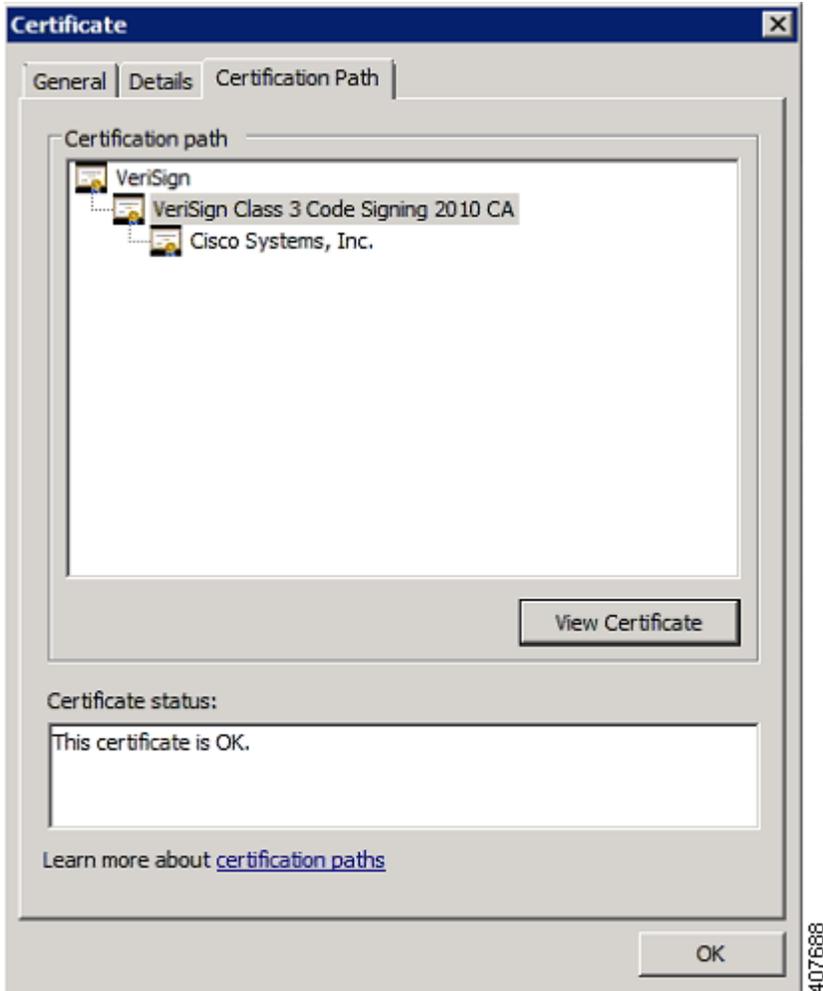


---

**Note** 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.

---

- b. Check the certificate chain:
- In the OVF Template Details window, click the **Cisco Systems, Inc.** hyperlink in the Publisher field.
  - In the Certificate window, click the **Certification Path** tab.
  - 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 **The certificate is OK**, as shown in the following figure.



---

## What To Do Next

Install Cisco EPN Manager 2.0 as described in [Install Cisco EPN Manager 2.0](#).



**Note** (OVA/VM automatic upgrades) If you are using this procedure to validate the `patching_upgrade.pl` script, return to [Step 7 of Perform an Automatic Upgrade \(High Availability\)](#) and run the script.

---

## 4 Install Cisco EPN Manager 2.0

- [Install Cisco EPN Manager Using an OVA/VM](#)
- [Install Cisco EPN Manager Using an ISO/Bare Metal Image](#)

### Install Cisco EPN Manager Using an OVA/VM

#### Overview of the OVA/VM Installation Process

1. Makes 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. [Install Cisco EPN Manager on the Server](#).
5. [Synchronize the Hardware and NTP Clocks](#).

#### Deploy the OVA from the VMware vSphere Client

##### Procedure

---

- 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, and verify the OVA file details including the product name, version, and size. Then click **Accept**.
- Step 6** In the Name and Location window:
- a. 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.
  - b. Select the configuration type as Standard or Professional based on your network size (see [System Requirements](#)).
  - c. 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**.



---

**Note** Cisco recommends you to select **Thick Provision Eager Zeroed** disk format. (There is also a **Thin Provision** choice, but it should only be used for lab or demo installations.)

---

- Step 10** Select the network mapping based on the configured IP address, then click **Next**.
- Step 11** In the Ready to Complete window:
- a. Verify your selections.
  - b. (Optional) If you want the virtual machine to automatically start after the OVA deployment finished, check the **Power on after deployment** check box.

c. 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 [Install Cisco EPN Manager on the Server](#).

## Install Cisco EPN Manager on the Server

### Procedure

**Step 1** If you did not specify that the virtual appliance should automatically start after deployment (in the previous procedure), manually start the VM. In the VMware vSphere client, right-click the deployed virtual appliance, then choose **Power > Power On**.

**Step 2** Click the **Console** tab, and at the localhost login prompt, enter **setup**.

**Step 3** 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.<br>The console will prompt you to add a secondary nameserver. Enter: <ul style="list-style-type: none"><li>• <b>Y</b> to enter a secondary nameserver.</li><li>• <b>N</b> to proceed to the next step of the installation.</li></ul>                                                                                       |
| 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 <b>time.nist.gov</b> ).<br>The console will prompt you to add a secondary NTP server. Enter: <ul style="list-style-type: none"><li>• <b>Y</b> to enter a secondary NTP server.</li><li>• <b>N</b> to proceed to the next step of the installation.</li></ul> |
| 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.<br>For a list of supported time zones, see the time zone reference in the <a href="#">Cisco Evolved Programmable Manager User and Administrator Guide</a> .                                                                                                                                                                       |
| Clock time            | The clock time (based on the selected System Time Zone).<br>The console will prompt you to change the system clock time. Enter: <ul style="list-style-type: none"><li>• <b>Y</b> to change the clock time.</li><li>• <b>N</b> to proceed to the next step of the installation.</li></ul>                                                                         |

| Parameter | Description                                                                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username  | The name of the first administrative user ( <b>admin</b> by default). This is the <b>Cisco EPN Manager CLI admin user</b> 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 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 4** 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 in a High Availability Deployment \(Fresh Installation\)](#).
  - Enter **no** if:
    - You are not using HA.
    - You are using HA but you want this server to be the primary server.



**Note** If any of the services do not start (such as the Health Monitor), right-click the virtual appliance and choose **Power > Restart Guest**.

- Step 5** Enter the 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 6** 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 7** (ISO/Bare Metal deployments) When the installation is complete:
- a. 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 in [Step 3](#).
  - b. Synchronize the hardware and NTP clocks as described in [Synchronize the Hardware and NTP Clocks](#).



**Note** Although this section is directed at OVA/VM installations, it includes information used when installing the product using an ISO/bare metal image.

- Step 8** (OVA/VM deployments) When the installation is complete, the virtual machine reboots and you are presented with a login prompt. Log in to the virtual appliance using the Cisco EPN Manager CLI admin username and password you configured in [Step 3](#).

## What To Do Next

Proceed to [Synchronize the Hardware and NTP Clocks](#).



**Note** If you are using this procedure to install Cisco EPN Manager on a secondary server as part of an automatic HA upgrade, return to [Step 15 in Perform an Automatic Upgrade \(High Availability\)](#) to continue the HA installation. This applies to both OVA/VM and ISO/bare metal automatic HA upgrades.

## Synchronize the Hardware and NTP Clocks

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

### Procedure

---

**Step 1** Log in as the Linux CLI root user as described in [How to Log In and Out as the Linux CLI User in Cisco EPN Manager 2.x: Complete Workflow](#). Be sure to use the procedures for Cisco EPN Manager 2.0.

**Step 2** Check the NTP service status and ensure that NTP has obtained a stable time reference using the following commands. You should see output similar to the examples below.

- a. Ensure that ntpd is running.

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

If ntpd (pid 3290) is not running, start it using the following command (and then verify it is running using the previous command):

```
service ntpd start
```

- b. 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.

```
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.
```

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

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

**Step 5** Check the output and ensure that the two clocks are synchronized (to at least within a few seconds of each other):

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

**Step 6** Log out as the Linux CLI users and restart Cisco EPN Manager services.

```
exit
exit
ncs stop
ncs start
```

---

## What To Do Next

Log in to the Cisco EPN Manager web GUI as described in [Get Started with Cisco EPN Manager](#).

# Install Cisco EPN Manager Using an ISO/Bare Metal Image

## Overview of the ISO/Bare Metal Installation Process

1. Makes 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. [Synchronize the Hardware and NTP Clocks](#).

## 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.

### Procedure

---

- 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 in to the Cisco IMC using the credentials that you entered [Step 7](#).
- 

## What To Do Next

Proceed to [Configure the Bare Metal Cisco UCS Server](#).

## Configure the Bare Metal Cisco UCS Server

### Procedure

---

- Step 1** From the left sidebar of the Cisco IMC web interface, click the **Storage** tab, and then click the **Cisco 12G SAS Modular Raid Controller (SLOT-HBA)** link.
- Step 2** In the Cisco 12G SAS Modular Raid Controller (SLOT-HBA) pane, click the **Controller Info** tab.
- Step 3** In the Actions area, click **Create Virtual Drive** from the **Unused Physical Drives** link.
- Step 4** In the Create Virtual Drive from Unused Physical Drives window, choose **10** from the RAID Level drop-down list.
- Step 5** In the Create Drive Groups area, select the physical drives listed under the Physical Drives area, then add them to the Drive Groups.
- Step 6** In the Virtual Drive Properties area, choose **Write Back Good BBU** from the Write Policy drop-down list.
- Step 7** Complete the required fields, then click **Create Virtual Drive**.
- Step 8** Click the **Virtual Drive Info** tab.
- Step 9** Click **Initialize**. A popup window is displayed.
- Step 10** Click **Initialize VD**.

- Step 11** Follow the steps below to enable Auto-Negotiation to speed up the installation:
- From the left sidebar, click the **Admin** tab.
  - Click **Network**.
  - In the Network pane, click the **Network Settings** tab.
  - In the Port Properties area, check the **Auto Negotiation** check box.
  - Click **Save Changes**.
- Step 12** From the left sidebar, click the **Admin** tab.
- Step 13** In the Utilities pane, click the **Actions** area, then click **Reboot Cisco IMC**.
- Step 14** Click **OK**.
- Step 15** When prompted, press **F2** to access the BIOS setup menu. The Aptio Setup Utility window appears, which provides the BIOS setup menu options.
- Step 16** In the Aptio Setup Utility window, click the **Boot Options** tab.
- Step 17** Enable **UEFI Boot options**, and then choose **Bus PCI RAID Adapter** for Boot Option #1.
- Step 18** Press **F10** to save and exit.
- The system is now prepared to boot from RAID. (For the first boot, however, you must do it from a remote virtual CD/DVD which is be 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

### Procedure

---

- Step 1** Power up the Cisco UCS Server.
- Step 2** Log in to Cisco IMC Server using the credentials you entered in [Step 7](#) in [Configure the Cisco IMC Server](#).
- Step 3** Choose **Server > Summary**, then click **Launch KVM Console** to open the console (in a separate window).
- 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.
- 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.
-

## 5 Upgrade from an Earlier Version of Cisco EPN Manager

These topics explain how to upgrade to Cisco EPN Manager 2.0 from an earlier version of Cisco EPN Manager.

- [Prerequisites for Upgrades](#)
- [Automatic Upgrade](#)
- [Backup-Restore Upgrade](#)
- [Post-Upgrade Tasks](#)

If you are performing an upgrade in a high availability deployment, see [Upgrade from an Earlier Version in a High Availability Deployment](#).

### Prerequisites for Upgrades

Check the following information before you begin the upgrade.

- Verify that your version of Cisco EPN Manager is supported for upgrade. See [Upgrade Options](#).
- Make sure 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 Cisco IMC.
- Back up your data. Refer to the backup topics 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](#)). You will need to use SCP to copy files from your client machine to the Cisco EPN Manager server.

### Automatic Upgrade

These are the basic steps of the automatic upgrade procedure:

1. Download the upgrade image and the patching upgrade script (and validation files) from Cisco.com to your client machine.
2. Copy the files from your client machine to the Cisco EPN Manager server.
3. Validate the `patching_upgrade.pl` script, then run the script. (The script ensures that optical devices are discovered correctly.)
4. Perform the upgrade.
5. Perform the post-upgrade licensing, authentication, and web GUI tasks described in [Post-Upgrade Tasks](#).

#### Before You Begin

Make sure you have completed the tasks in [Prerequisites for Upgrades](#).

#### Procedure

- 
- Step 1** From the [Software Download site on Cisco.com](#), locate and download the following files to your client machine.
- CEPNM upgrade image—Contains the upgrade image. 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.
  - Patching Upgrade zip file—Contains the `patching_upgrade.pl` script, which ensures that optical devices are discovered correctly. You will run this script before performing the upgrade.
  - Patching Upgrade signature file—Contains the `patching_upgrade.pl.signature` file, which you will use to validate the `patching_upgrade.pl` script.
  - Cisco EPNM 2.0 pem file—Contains the `CiscoEPNM 2.0.pem` file, which you will use to validate the `patching_upgrade.pl` script.

**Step 2** After the download completes, compare the upgrade image's size on the Software Download site with its size on your client machine. 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.

- a. Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
- b. Log in as the Linux CLI root user as described in [How to Log In and Out as the Linux CLI User in Cisco EPN Manager 1.2.x: Complete Workflow](#). Be sure to use the procedures for Cisco EPN Manager 1.2.x.
- c. Verify that `/localdisk/defaultRepo` has enough space using the following command. If it does not, delete all files and directories to free up some space.

```
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`). You should 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 upgrade file client machine

For example (the following command is one line):

```
scp jsmith@123.456.789.101:/temp/CEPNM-Upgrade-3.0.X_to_3.1.0.0.132.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** Validate the `patching_upgrade.pl` script. (That script ensures that optical devices are discovered correctly.)

- a. Make sure you are logged in as the Linux CLI root user.
- b. In the `/localdisk/defaultRepo` directory, unzip the Patching Upgrade zip file:  

```
unzip patching_upgrade.zip
```
- c. Verify that these three files are in `/localdisk/defaultRepo`:
  - `patching_upgrade.pl`
  - `patching_upgrade.pl.signature`
  - `CiscoEPNM 2.0.pem`
- d. Validate the `patching_upgrade.pl` script by starting at [Step 3](#) in the procedure [Verify the ISO Image or OVA Package](#). If the result of the `openssl` command `Verified OK`, proceed to the next step. Otherwise, repeat the download procedure.

**Step 7** Run the Patching Upgrade script:

```
perl patching_upgrade.pl
```

**Step 8** Log out as the Linux CLI root user.

```
su admin
```

**Step 9** Stop the server.

```
ncs stop
```

**Step 10** Upgrade the Cisco EPN Manager software using the upgrade file that is located in /localdisk/defaultRepo. 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.

```
application upgrade filename defaultRepo
```

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

```
application upgrade CEPNM-Upgrade-3.0.X_to_3.1.0.0.132.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
```

---

## What To Do Next

Perform the tasks in [Post-Upgrade Tasks](#).

## Backup-Restore Upgrade

### Before You Begin

- Make sure you have completed the tasks in [Prerequisites for Upgrades](#).
- 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.

### Procedure

- 
- Step 1** On the new server, install Cisco EPN Manager 2.0 by following the steps in [Install Cisco EPN Manager 2.0](#).
  - 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](#).

## 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](#).
- Instruct user 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 by referring to the user management topics in the [Cisco Evolved Programmable Network Manager User and Administrator Guide](#).

## 6 High Availability

- [High Availability Deployment Models](#)
- [High Availability Installation Considerations](#)
- [Prerequisites for High Availability Installations](#)
- [Install Cisco EPN Manager in a High Availability Deployment \(Fresh Installation\)](#)
- [Upgrade from an Earlier Version in a High Availability Deployment](#)

### High Availability Deployment Models

Cisco EPN Manager HA feature supports the following three HA deployment models.

| HA Deployment Model | In this deployment, both servers are located: | Example:                                                 |
|---------------------|-----------------------------------------------|----------------------------------------------------------|
| Local               | On 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—Remote HA deployments are least likely to be affected by natural disaster, resulting in a less complex and costly business continuity model. While the same is true for Campus HA deployments, this can complicate business continuity planning and increase disaster recovery. Local HA deployments are most vulnerable to disaster because of server co-location, which can result in increased insurance costs.
- 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 fallback. It also allows both the primary and secondary servers to share a common management IP address.
- Bandwidth/latency—Bandwidth/latency is best for 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/latency than Local HA deployments. Remote HA deployments have the least bandwidth.
- 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.

### High Availability Installation Considerations

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

- The framework requires at least 1 Gb per second of network bandwidth is required to handle HA operations. 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 framework requires net latency 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.

HA performance is always sensitive to the net throughput delivered by the network that connects the primary and secondary servers. This restriction applies (to at least 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. But 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.

## 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 the 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 is automatically switches back to the primary server. For more details about HA, see the [Cisco Evolved Programmable Network Manager User and Administrator Guide](#).

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.

## Prerequisites for High Availability Installations

- Make sure your hardware and software 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 Cisco IMC.
- Make sure the secondary server is configured as follows:
  - The secondary server must have hardware and software specifications that meet or exceed the requirements for your primary server. For example, if you installed Cisco EPN Manager on the primary server and specified the Standard system size, your secondary server (1) must also be installed using the Standard system size, and (2) must meet or exceed all requirements for Standard-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, the secondary server must be on the same subnet as the primary server (it must be a Local HA deployment).
- Your network should meet these requirements:
  - Your network has at least 1 Gb per second of network bandwidth on the link between the two servers, with the lowest latency achievable (otherwise data replication may be impacted).
  - If there is a firewall between the primary and secondary servers, you have permission from the firewall for the ports used by HA. The ports are listed in [Ports Used by Cisco EPN Manager](#).
- You have the following information, which you will need to enter during the installation:
  - The 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. 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 in a High Availability Deployment (Fresh Installation)

### Before You Begin

Make sure your servers meet the requirements listed in [Prerequisites for High Availability Installations](#).

### Procedure

- 
- Step 1** Install Cisco EPN Manager on the primary server as described in [Install Cisco EPN Manager 2.0](#). You should perform the entire procedure.
  - Step 2** Install Cisco EPN Manager on the secondary server as described in [Install Cisco EPN Manager 2.0](#).
  - Step 3** When you are prompted to choose whether you want this newly-installed server to act as a secondary fallback 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 in [Step 11](#). (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. When the installation is complete, the VM (OVA/VM) or Cisco UCS server (ISO/bare metal) will reboot.
  - Step 7** When you are presented with a login prompt, log in using the Cisco EPN Manager CLI admin username and password you specified in [Step 3 of Install Cisco EPN Manager on the Server](#).
  - Step 8** Verify that all processes are running on the secondary server using the **ncs status** command.
  - 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** If you used this procedure to install Cisco EPN Manager on your servers as part of a backup-restore upgrade, go to [Step 4 in Perform a Backup-Restore Upgrade \(High Availability\)](#).
  - Step 11** 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](#).
-

# Upgrade from an Earlier Version in a High Availability Deployment

- [Prerequisites for Upgrade in a High Availability Deployment](#)
- [Perform an Automatic Upgrade \(High Availability\)](#)
- [Perform a Backup-Restore Upgrade \(High Availability\)](#)

## Prerequisites for Upgrade in a High Availability Deployment

Before you begin, ensure that:

- Your current version Cisco EPN Manager is supported for upgrade. See [Upgrade Options](#).
- You have the password (authentication key) that was created when HA was enabled. You will need it to perform the Cisco EPN Manager 2.0 installation on the secondary server.
- Your data has been backed up. Refer to the backup topics in *Cisco Evolved Programmable Network Manager User and Administrator Guide*.
- No backups are in progress.
- Your client machine is running SCP. You will need to use one of these to copy files from your client machine to the Cisco EPN Manager server.

## Perform an Automatic Upgrade (High Availability)

These are the basic steps of the automatic upgrade procedure:

1. Download the upgrade image and the patching upgrade script (and validation files) from Cisco.com to your client machine.
2. Copy the files from your client machine to the Cisco EPN Manager server.
3. Validate the `patching_upgrade.pl` script, then run the script.
4. Perform the upgrade.
5. Perform the post-upgrade licensing, authentication, and web GUI tasks described in [Post-Upgrade Tasks](#)

### 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 Upgrade in a High Availability Deployment](#).

### Procedure

---

- Step 1** On the primary server, note the HA configuration, then remove it.
- a. Log into Cisco EPN Manager as a user with Administrator privileges.
  - b. Choose **Administration > Settings > High Availability**.
  - c. Make note of the HA configuration. You will need this information to reconfigure HA after the upgrade.
  - d. Choose **HA Configuration** in the left navigation area, then click **Remove**.
  - e. Wait for the remove operation to complete.
  - f. 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 following files to your client machine
- CEPNM upgrade image—Contains the upgrade image. 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.
  - Patching Upgrade zip file—Contains the `patching_upgrade.pl` script, which ensures that optical devices are discovered correctly. You will run this script before performing the upgrade.

- Patching Upgrade signature file—Contains the **patching\_upgrade.pl.signature** file, which you will use to validate the `patching_upgrade.pl` script.
- Cisco EPNM 2.0 pem file—Contains the **CiscoEPNM 2.0.pem** file, which you will use to validate the `patching_upgrade.pl` script.

**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.

- Start an SSH session with the primary Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
- Log in as the Linux CLI root user as described in [How to Log In and Out as the Linux CLI User in Cisco EPN Manager 1.2.x: Complete Workflow](#). Be sure to use the procedures for Cisco EPN Manager 1.2.x.
- Verify that `/localdisk/defaultRepo` has enough space using the following command. If it does not, delete all files and directories to free up some space.

```
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.

```
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 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-3.0.X_to_3.1.0.0.132.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** Validate the **patching\_upgrade.pl** script on the primary server. (That script ensures that optical devices are discovered correctly.)

- Log in as the Linux CLI root user as described in [How to Log In and Out as the Linux CLI User in Cisco EPN Manager 1.2.x: Complete Workflow](#). Be sure to use the procedures for Cisco EPN Manager 1.2.x.
- In the `/localdisk/defaultRepo` directory, unzip the Patching Upgrade zip file:

```
unzip patching_upgrade.zip
```

- c. Verify that these three files are in /localdisk/defaultRepo:
  - patching\_upgrade.pl
  - patching\_upgrade.pl.signature
  - CiscoEPNM 2.0.pem
- d. Validate the patching\_upgrade.pl script by starting at [Step 3](#) in the procedure [Verify the ISO Image or OVA Package](#). If the result of the openssl command Verified OK, proceed to the next step. Otherwise, repeat the download procedure.

**Step 10** Run the Patching Upgrade script:

```
perl patching_upgrade.pl
```

**Step 11** On the primary server, log out as the Linux CLI root user.

```
su admin
```

**Step 12** Stop the primary server.

```
ncs stop
```

**Step 13** Upgrade the primary server using the upgrade file that is located in /localdisk/defaultRepo. 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.

```
application upgrade filename defaultRepo
```

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

```
application upgrade CEPNM-Upgrade-3.0.X_to_3.1.0.0.132.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
```

This step can take 30 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 14** Install Cisco EPN Manager 2.0 on the secondary server (you will perform a fresh installation on this server):

- OVA/VM installation—Perform the steps in these sections:
  - [Deploy the OVA from the VMware vSphere Client](#)
  - [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:
  - [Configure the Cisco IMC Server](#)
  - [Configure the Bare Metal Cisco UCS Server](#)
  - [Install Cisco EPN Manager on the Server](#)

**Step 15** Log into the secondary server as a Cisco EPN Manager CLI admin user and restart the secondary server by running the following command:

```
ncs start
```

**Step 16** On the primary server:

- a. Verify that the server is restarted.
- b. Run the `ncs status` command and make sure that the Health Monitor process and other processes have restarted.

**Step 17** If the `ncs status` output on the primary server lists **Compliance engine is stopped**, do the following:

- a. Stop Cisco EPN Manager.

```
ncs stop
```

- b. Log in as the Linux CLI root user (see [How to Log In and Out as the Linux CLI User in Cisco EPN Manager 2.x: Complete Workflow](#)). Be sure to use the procedures for Cisco EPN Manager 2.x.

- c. 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 18** On the secondary server:

- a. Verify that the server is restarted.
- b. Run the `ncs status` command and make sure that the Health Monitor process and other processes have restarted.

**Step 19** Perform the following post-upgrade tasks on the primary server:

- 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](#).
- Instruct user 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 by referring to the user management topics in the [Cisco Evolved Programmable Network Manager User and Administrator Guide](#).

**Step 20** 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](#).

---

## Perform a Backup-Restore Upgrade (High Availability)

For an HA backup-restore upgrade, you will perform the following steps:

1. Remove HA.
2. Back up your data to a remote repository.
3. Perform a fresh installation of CEPNM 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 Upgrade in a High Availability Deployment](#).
- 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.

## Procedure

- Step 1** On the primary server, remove the High Availability configuration:
- Log into Cisco EPN Manager as a user with Administrator privileges.
  - Choose **Administration > Settings > High Availability**.
  - Make note of the HA configuration. You will need this information to reconfigure HA after the upgrade.
  - Choose **HA Configuration** in the left navigation area, then click **Remove**.
  - Wait for the remove operation to complete.
  - 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 2.0 on the two new servers as described in [Install Cisco EPN Manager in a High Availability Deployment \(Fresh Installation\)](#).
- 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:
- Verify that the server is restarted.
  - Run the `ncs status` command and make sure that the Health Monitor process and other processes have restarted.

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

- Stop Cisco EPN Manager.  
`ncs stop`
- Log in as the Linux CLI root user (see [How to Log In and Out as the Linux CLI User in Cisco EPN Manager 2.x: Complete Workflow](#)). Be sure to use the procedures for Cisco EPN Manager 2.x.
- 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 following 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](#).
  - Instruct user 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 by referring to the user management topics in the [Cisco Evolved Programmable Network Manager User and Administrator Guide](#).

- 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](#).
- 

## 7 Get Started with Cisco EPN Manager

- [Log In to the Cisco EPN Manager Web GUI](#)
- [Navigation to Common Tasks](#)

### Log In to the Cisco EPN Manager Web GUI

Follow these steps to log in to 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 in [Step 5 of Install Cisco EPN Manager on the Server](#). 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:
- Change the password for the web GUI root user by choosing **Administration > Users > Roles & AAA > Change Password**.
  - 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](#).
  - 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, see the [Cisco Evolved Programmable Network Manager User and Administrator Guide](#).

## Navigation to Common Tasks

The following table lists common Cisco EPN Manager tasks, their navigation in the web GUI, and where to get more information.

| <b>Task</b>                                          | <b>Navigation in Cisco EPN Manager</b>                                        | <b>Chapter/Section in Cisco EPN Manager User and Administrator Guide</b>                                |
|------------------------------------------------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Discovering your network                             | Inventory > Device Management > Network Devices                               | <i>Add and Organize Devices/Add Devices to Cisco EPN Manager</i>                                        |
| Setting up monitoring                                | Monitor > Monitoring Tools > Monitoring Policies                              | <i>Monitor Device and Network Health and Performance/How Device Health and Performance Is Monitored</i> |
| Setting up virtual domains to control device access  | Administration > Users > Virtual Domains                                      | <i>User Permissions and Device Access/Create Virtual Domains to Control User Access to Devices</i>      |
| Using monitoring dashboards                          | Dashboard > Overview                                                          | <i>Get Started with Cisco EPN Manager /Set Up and Use the Dashboards</i>                                |
| Using templates for configuring features and devices | Configuration > Templates > Features and Technologies                         | <i>Create Templates To Automate Device Configuration Changes</i>                                        |
| Viewing alarms                                       | Monitor > Monitoring Tools > Alarms and Events                                | <i>Monitor Alarms and Events</i>                                                                        |
| Comparing and maintaining device configurations      | Inventory > Device Management > Configuration Archive                         | <i>Manage Device Configuration Files</i>                                                                |
| Maintaining software image files                     | Inventory > Device Management > Software Images                               | <i>Manage Device Software Images</i>                                                                    |
| Managing users                                       | Administration > Users > Users, Roles & AAA                                   | <i>User Permissions and Device Access/Add Users and Manage User Accounts</i>                            |
| Viewing the network using Network Topology maps      | Maps > Topology Maps > Network Topology                                       | <i>Visualize the Network Topology/Use Network Topology Maps</i>                                         |
| Viewing the network using Geographical Maps          | Maps > Topology Maps > Network Topology, then click the Geographical Map icon | <i>Visualize the Network Topology/Use Geographical Maps</i>                                             |
| Provisioning services                                | Maps > Topology Maps > Network Topology > Circuits/VCS                        | <i>Provision Circuits/VCS</i>                                                                           |

## 8 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](#).

## Procedure

---

**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.

## 9 Related Documentation

Refer to the *Cisco Evolved Programmable Network Manager 2.0 Documentation Overview* for information about and links to all of the documentation that is provided with Cisco EPN Manager 2.0 and its maintenance packs.



**Note** We sometimes update the documentation after original publication. Therefore, you should also review the documentation on [Cisco.com](http://www.cisco.com) for any updates.

---

## 10 Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at: <http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015-2016 Cisco Systems, Inc. All rights reserved

