Cisco EPN Manager 6.0 Installation

This chapter provides the information required for planning your installation of Cisco EPN Manager 6.0 and ensuring that you meet all the prerequisites required for the installation. It also provides procedures for installing Cisco EPN Manager 6.0 in a standard, non-high availability environment. For high availability, see Cisco EPN Manager 6.0 High Availability Installation.

Note Cisco EPN Manager software is distributed with all the components necessary for its optimized and secure operation, including the Red Hat Linux operating system and the Oracle database. All security-related configurations, regression testing, performance, and scalability metrics are based on the set of components and configurations included in the original Cisco EPN Manager software distribution. Cisco provides periodic EPN Manager software updates that can also contain necessary updates to the packages installed on the operating system or to the database.

Note that if any of the following changes are made to the original distributed Cisco EPN Manager software, Cisco will no longer support the operating environment:

- Configuration changes to the software or operating system, or installation of other components that are not part of the original distribution.

- Direct installation and application of third-party software on the Red Hat Linux operating system embedded within Cisco EPN Manager.

- Application of updates or patches that are **not** provided by Cisco to individual Cisco EPN Manager components.

- Changes to the internal Cisco EPN Manager settings that are not documented as modifiable in the Cisco EPN Manager User and Administrator Guide on Cisco.com, as these changes may weaken security, disable functionality, or degrade scalability and performance.

This chapter contains the following sections:

Installation Overview

Cisco EPN Manager 6.0 can be installed as a fresh installation either on a virtual machine or a bare metal server. If you are already using a previous version of Cisco EPN Manager, you can upgrade to Cisco EPN Manager 6.0 and thereby retain your data.

Note Bare Metal: Although still available in current release, Bare Metal installation has been deprecated in release 5.0.1 and will be removed from release 6.1 onwards. Cisco strongly recommends you to install release 6.0 on VMvare. Upgrade to upcoming release 6.1 will not be possible if you install release 6.0 on Bare Metal.

The following topics provide an overview of the Cisco EPN Manager 6.0 installation and upgrade options and provide additional useful installation-related information.

- Installation Options
- Upgrade Options
- High Availability Overview
- Users Created During Installation

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

Installation Options

You can install Cisco EPN Manager 6.0 either on a virtual machine (VM) or a bare metal server:

- OVA/VMWare VM installation—For a VM installation, install the Open Virtual Appliance (OVA) file on a dedicated server that complies with the requirements listed in OVA/VM Requirements. We recommend that you run only one Cisco EPN Manager VM instance per server hardware.

- ISO/bare metal installation—For a bare metal server installation, install the ISO image, which acts as a virtual boot that supports the Cisco Unified Computing System (UCS) server installation. The requirements are listed in Bare Metal Requirements (Deprecated). You can also use the ISO image to install Cisco EPN Manager on a VM. A built-in terminal or console server application called Cisco Integrated Management Controller (Cisco IMC) is used to install Cisco EPN Manager on the bare metal Cisco UCS server hardware.

Note For Cisco EPN Manager 6.0 installation on a bare metal server or any server that is installed in UEFI (EFI) mode rather than Legacy BIOS mode, please ensure you follow the mandatory steps given below:

1. In CEPNM admin CLI, switch to shell: **$ shell**.

2. Switch to root: **$ sudo -i**.

3. Extract the zip file, which contains official RH rpms: **$ mkdir rpms; cd rpms**.

4. Unzip the grub2_packages.zip file.

5. Install the files using: **$ rpm -Uvh *.rpm —force**.

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

OVA and ISO installations include the following:

- Red-Hat Enterprise Linux 7.9 operating system

- Oracle Database 19c Enterprise Edition Release 19.13.0.0.0

- EPN Manager

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

Firmware Upgrade

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

Upgrade Options

You can upgrade to Cisco EPN Manager 6.0 by following the valid upgrade path relevant for your existing deployment. See Valid Upgrade Paths.

The following methods are available for upgrading to Cisco EPN Manager 6.0:

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

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

Users Created During Installation

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

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

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

  ```
  admin# change-password
  ```

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

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

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

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

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

System Requirements

The following sections list the requirements that must be met before installing Cisco EPN Manager 6.0:

- Hardware and Software Requirements
- Web Client Requirements
- Ports Used by Cisco EPN Manager

Hardware and Software Requirements

- OVA/VM Requirements
- Bare Metal Requirements (Deprecated)

OVA/VM Requirements

The following table summarizes the OVA/VM system requirements:

- **Extended:** Recommended for scale network configuration in production environments.
- **Professional:** Recommended for non-scale network configuration in production environments.

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

It is not recommended to use the Very-Large profile. It is only intended to be used when requested by Cisco TAC and not supposed to be used in standard installations.

Note External storage is supported for OVA/VM installations.

Server Type	Item	Extended	Professional
Virtual Machine	VMWare ESXi version **Note** Installations using an OVA image are supported on VMWare ESXi, on your own hardware. In all cases your server must meet or exceed the requirements listed in this table.	6.5, 6.7, 7.0.1	6.5, 6.7, 7.0.1
	Appliance image format	OVA	OVA

Server Type	Item	Extended	Professional
Hardware	Virtual CPU (vCPU)	24	16
	Memory (DRAM)	128 GB	64 GB
	Disk Capacity **Note** Reported disk size does not consider RAID configurations.	4 TB	2.8 TB
	Disk I/O speed	Minimum: Greater than 900 MBPS Full Scale: Greater than 1150 MBPS	Minimum: Greater than 700 MBPS Full Scale: Greater than 900 MBPS

Bare Metal Requirements (Deprecated)

Note   Bare Metal: Although still available in current release, Bare Metal installation has been deprecated in release 5.0.1 and will be removed from release 6.1 onwards. Cisco strongly recommends you to install release 6.0 on VMvare. Upgrade to upcoming release 6.1 will not be possible if you install release 6.0 on Bare Metal.

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

External storage is not supported for bare metal installations.

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

Bare Metal Requirements for Minimum and Recommended Deployments (No High Availability)

These are the requirements for minimum and recommended deployments (no high availability).

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

Hardware	Deployment Type	Minimum	Recommended
	Cisco UCS server type	Cisco UCS C220 M4, M4S, M5, M5SX and M5L	Cisco UCS C220 M4, M4S, M5, M5SX and M5L
	CPU (cores/threads)	1 x CPU (10 C/20 T)	2 x CPU (10 C/20 T)
	Memory	64 GB	128 GB
	Disk capacity	2.8 TB after RAID	4 TB after RAID
	Disk I/O speed	Minimum: 700 MBps Recommended: 900 MBps	Minimum: 900 MBps Recommended: 1150 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.

Hardware	Requirement
Cisco UCS server type	Cisco UCS C220 M4, M4S, M5, M5SX, and M5L
CPU speed	Intel(R) Xeon(R) CPU E5-2650 v3 @ 2.30GHz or above
Cores/threads	10 C/20 T
Storage adapter	Cisco 12G SAS Modular Raid Controller
Hard Disk	Product ID: Cisco 12G SAS Modular Raid Controller
Interface	SATA (Serial Advanced Technology Attachment)
Hardware Sector Size	512 Native, 4K sector disk
Memory	64 GB
RAID level	RAID 10
Number of NICs	1
Disk capacity	4x900 GB
Virtual hard disk size in RAID controller	1 TB (minimum requirement)
Hard disk controller location	Slot 1
Hard disk I/O speed	450 MBps
Hard disk RPM	Minimum 15k RPM SAS (flash recommended)

Hardware	Requirement
Network bandwidth	Ideal: 977 Mbps Minimum: 500 Mbps or more
Latency	Less than 100 msecs

Web Client Requirements

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

- Hardware—Mac or Windows laptop or desktop compatible with one of the tested and supported browsers listed below.

- Browsers:

Note You can have upto three Cisco EPN Manager tabs open simultaneously in a single browser session.

- Google Chrome versions 70 onwards

- Mozilla Firefox ESR version 78

- Mozilla Firefox versions 70 onwards

- Microsoft Internet Explorer (IE) 11.0 is not supported

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

To improve loading time and reduce network bandwidth usage, Cisco EPN Manager caches static files (js, css) in the browser in the same version of Cisco EPN Manager (Firefox and IE browsers).

Note Google Chrome ignores all caching directives and reloads page content because of known limitations regarding self-signed certificates.

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.

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

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

Port	Protocol	Usage	Safe to Disable?	Notes
21	TCP	To transfer files to and from devices using FTP.	Yes	Disable FTP from the web GUI under **Administration > Settings > System Settings**, then choose **General > Server**. After disabling FTP, as the CLI admin user, stop and restart the server.
22	TCP	To initiate SSH connections with the Cisco EPN Manager server, and to copy files to the Cisco EPN Manager server using SCP or SFTP.	Depends	Only if alternative protocols like SCP or SFTP or HTTPS are used for image distribution, and if supported by the managed devices.
69	UDP	To distribute images to devices using TFTP.	Depends	This might be still needed by older managed devices that only support TFTP and not SFTP or SCP.
162	UDP	To receive SNMP traps from network devices.	No	—
443	TCP	For browser access to the Cisco EPN Manager server via HTTPS.	No	—
514	UDP	To receive syslog messages from network devices.	No	—
1522	TCP	For High Availability (HA) communication between active and standby Cisco EPN Manager servers. Used to allow Oracle JDBC traffic for Oracle database synchronization.	Yes	If at least one Cisco EPN Manager server is not configured for HA, this port is automatically disabled.
2021	TCP	To distribute images to devices using FTP.	No	—

| Port	Protocol	Usage	Safe to Disable?	Notes
8082	TCP	For the HA Health Monitor web interface (via HTTP). Used by primary and secondary servers to monitor their health status via HTTP.	No (If HA configured)	—
8085	TCP	Used by the Health Monitor process to check network bandwidth speed between primary and secondary servers,when the user executes readiness test under high availability.	No (If HAconfigured)	—
8087	TCP	To update software on the HA secondary backup server (uses HTTPS as transport).	No	—
9991	UDP	To receive Netflow data packets.	Yes	Cisco EPN Manager does not support Netflow. You should disable this traffic in the network firewall.
9992	TCP	To manage M-Lync using HTTP or HTTPS.	Yes	Cisco EPN Manager does not support M-Lync. You should disable this traffic in the network firewall.
11011 to 11014	TCP	For PnP operations for proprietary Cisco Network Service (CNS) protocol traffic.	Yes	Cisco EPN Manager does not support PnP. You should disable this traffic in the network firewall by entering the following commands in this sequence (as the Cisco EPN Manager CLI admin user): **ncs pnp-gateway disable** **ncs stop** **ncs start**

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

Table 2: Destination Ports Used by Cisco EPN Manager

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

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

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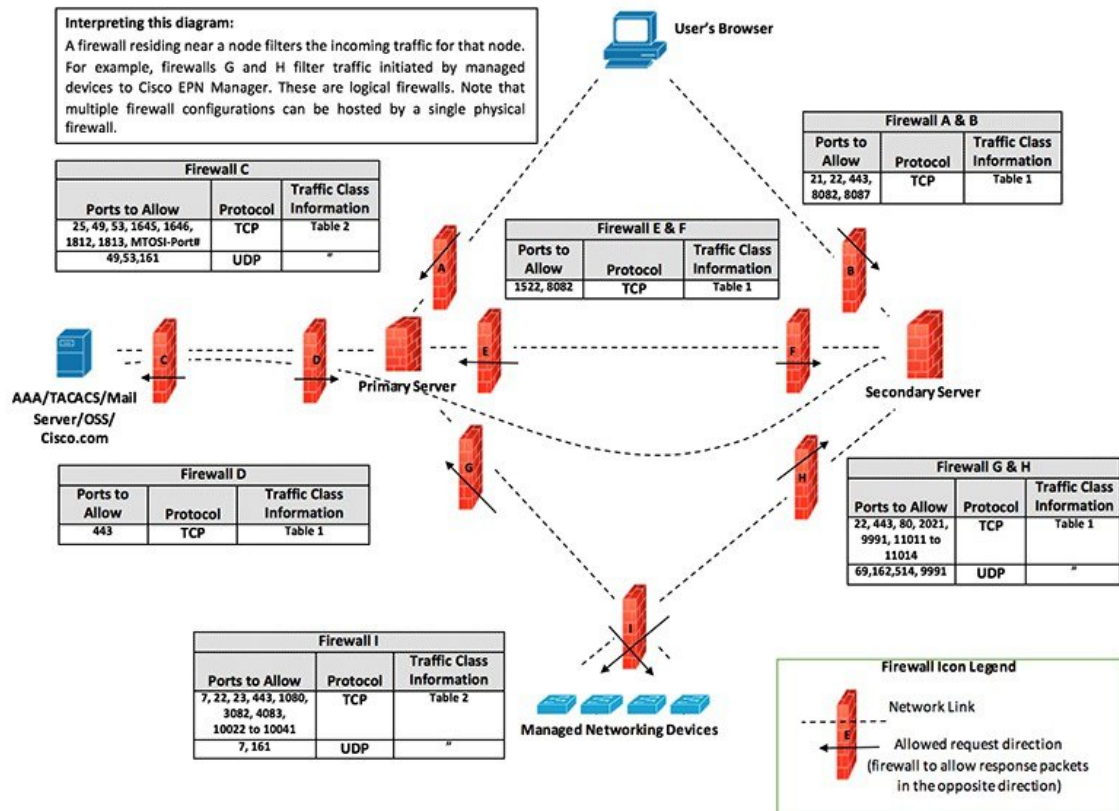
Installation Prerequisites

Licensing

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

For a production environment:

- Base license (required)

- Standby license (optional)—Obtain this license if you will have a high availability deployment with two Cisco EPN Manager servers configured in a redundancy configuration.

- Right-to-Manage licenses for the types and corresponding numbers of devices to be managed by Cisco EPN Manager.

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

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

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

Prerequisites for OVA/VM Installations

Before installing Cisco EPN Manager, ensure that:

- Your deployment meets the general hardware and software requirements listed in System Requirements, and specifically in OVA/VM Requirements.
- Hardware resources are reserved for the Cisco EPN Manager server to ensure optimal performance. CPU minimum clock is 2.2 Ghz per CPU.

- VMware 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 ESXi host is reachable.
- The Cisco EPN Manager OVA is saved to the same machine where vSphere web interface is launched.
- The downloaded OVA package has been verified as described in Verify the ISO Image or OVA Package.

Prerequisites for ISO/Bare Metal Installations (Deprecated)

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

- Your deployment meets the general hardware and software requirements listed in System Requirements, and specifically in Bare Metal Requirements (Deprecated).
- The following software is installed:

  - Java with JRE Version 1.7.0
  - Flash Driver v9.0.246 or higher
  - The minimum web browser version required for HTML5 KVM is Chrome 45, Firefox 45, IE 11, Opera 35, and Safari 9.

- The downloaded ISO image has been verified as described in Verify the ISO Image or OVA Package.
- A reliable link is available for accessing the installation file. VPN links are not recommended.

Verify the ISO Image or OVA Package

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

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

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

- The Cisco EPN Manager 6.0 product OVA package or ISO image to be verified (*.iso or *.ova)

- The Cisco EPN Manager 6.0 OVA or ISO signature file (*.signature)

- The Cisco EPN Manager 6.0 certificate file (*.pem)

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

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

Step 4 Run the following command:

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

Where:

- *cert-file* is the certificate file (*.pem)

- *sig-file* is the signature file (*signature)

- *product-file* is the file to be verified

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

- For an OVA package, proceed to *Step 6*.

- For an ISO file, go to Install Cisco EPN Manager 6.0 (No HA).

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

a. Verify that Cisco Systems is the publisher:

1. In the VMware vSphere client, choose **File > Deploy OVF Template**.

2. Browse to the OVA installation file (*.ova) and select it, then click Next.

3. Check whether the Publisher field in the OVF Template Details window displays **Cisco Systems, Inc** with a green check mark next to it. Do not proceed if the Publisher field displays **No certificate present**. This indicates that the image is not signed or the file is not from Cisco Systems or the file has been tampered with. Contact your Cisco representative.
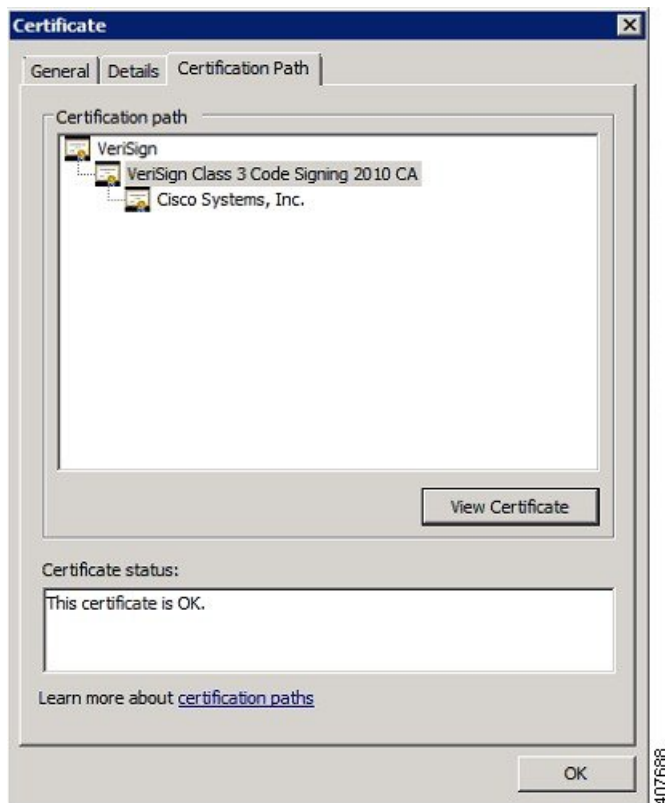
Note Do not validate the image using the information in the Vendor field. This field does not authenticate Cisco Systems as the publisher.

b. Check the certificate chain:

c. In the OVF Template Details window, click the **Cisco Systems, Inc.** hyperlink in the Publisher field.

d. In the Certificate window, click the **Certification Path** tab.

e. In the Certification Path tab (which lists the certificate chain), ensure that the Certification Path area displays **Cisco Systems, Inc.** and the Certificate Status displays **This certificate is OK**, as shown in the following figure.

Certificate

General | Details | Certification Path

Certification path

VeriSign
└─ VeriSign Class 3 Code Signing 2010 CA
   └─ Cisco Systems, Inc.

View Certificate

Certificate status:

This certificate is OK.

Learn more about certification paths

OK

407688

Install Cisco EPN Manager 6.0 (No HA)

- Install Cisco EPN Manager Using an OVA/VM
- Install Cisco EPN Manager Using an ISO on Bare Metal Image (Deprecated)
- Start Cisco EPN Manager Setup Process

Install Cisco EPN Manager Using an OVA/VM

1. Make sure your deployment meets the requirements in System Requirements.

2. Make sure your deployment meets the prerequisites in Prerequisites for OVA/VM Installations. This includes verifying the OVA package.

3. Deploy the OVA from the VMware vSphere Client.

4. Set the System Time of the Deployed OVA

5. Start Cisco EPN Manager Setup Process.

Deploy the OVA from the VMware vSphere Client

Step 1 Launch the VMware vSphere client.

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

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

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

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

Step 6 In the Name and Location window:

  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 Professional, Extended or Very-Large 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**, then click **Next**.

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

Step 11 In the Ready to Complete window:

  a. Verify your selections.

  b. (Optional) If you want the virtual machine to automatically start after the OVA deployment has 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 .

Set the System Time of the Deployed OVA

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

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

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

Step 4 Click **Save**.

Step 5 Boot the VM.

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

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

What to do next

Proceed to Start Cisco EPN Manager Setup Process.

Install Cisco EPN Manager Using an ISO on Bare Metal Image (Deprecated)

1. Make sure your deployment meets the requirements in System Requirements.
2. Make sure your deployment meets the prerequisites in Prerequisites for ISO/Bare Metal Installations (Deprecated). 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.

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

Configure the Cisco IMC Server

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

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

Step 2   Power on the Cisco UCS server.

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

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

- DHCP Enabled—Select this option to enable DHCP for dynamic network settings. Before you enable DHCP, your DHCP server must be preconfigured with the range of MAC addresses for this server.

- Cisco IMC IP—Enter the IP address of Cisco IMC.

- Subnetmask—Enter the subnet mask to append to the Cisco IMC IP address. It must be in the same subnet as the host router.

- Gateway—Enter the IP address of the default gateway router.

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

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

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

• Username: **admin**

• Password: **password**

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

Step 9   Update the following fields as specified:

• NIC mode—Select **Dedicated**.

• IP (Basic)—Select **IPV4**.

• DHCP—Disable DHCP if enabled.

• CIMC IP—Enter the IP address of the Cisco IMC.

• Prefix/Subnet—Enter the subnet of the Cisco IMC.

• Gateway—Enter the gateway address.

• Pref DNS Server—Enter the preferred DNS server address.

• NIC Redundancy—Null.

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

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

• Hostname—Enter the Cisco IMC hostname.

• Dynamic DNS—**Disable**.

• Enter the admin password. If you leave the Password field blank, the default password is **password**.

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

Step 13   Open a browser and enter the following URL:

https://*Cisco IMC_IP_address*

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

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

What to do next

Proceed to Configure the Bare Metal Cisco UCS Server.

Configure the Bare Metal Cisco UCS Server

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

Note   Disable any SD card controller, such as FlexFlash before installing EPNM.

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

a) From the left sidebar of the Cisco IMC web interface, choose **Chassis > Summary**.

b) Change the time zone to the correct *local* time zone.

c) Launch KVM and connect to the server.

d) Reset the server (warm boot).

e) When prompted, press F2 to enter CMOS.

f) Change the time to the current UTC time (not the local time) and press F10 to save your change.

g) **For UCS C220 M4 devices only:**Click the **Boot Options** tab. Enable **UEFI Boot options**, and then choose **Bus PCI RAID Adapter** for Boot Option #1.

h) Reboot the host.

i) Reboot Cisco IMC and log in again.

j) Check that the time is correct in **Chassis > Summary**.

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

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

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

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

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

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

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

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

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

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

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

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

a. From the left sidebar, click the **Admin** tab.

b. Click **Network**.

c. In the Network pane, click the **Network Settings** tab.

d. In the Port Properties area, check the **Auto Negotiation** check box.

e. Click **Save Changes**.

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

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

Step 16   Click **OK**.

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

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

What to do next

Proceed to Install Cisco EPN Manager from an ISO Image.

Install Cisco EPN Manager from an ISO Image

Step 1   Power up the Cisco UCS Server.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Step 14   Go to *Step 3* in Start Cisco EPN Manager Setup Process to complete the installation.

Start Cisco EPN Manager Setup Process

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

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

Parameter	Description
Hostname	Host name of the virtual machine.
IP Address	IP address of the virtual machine.

Parameter	Description
IP default netmask	Default subnet mask for the virtual machine IP address.
IP default gateway	IP address of the default gateway.
Default DNS domain	Default DNS domain name.
Primary nameserver	IP address of the primary DNS server. The console will prompt you to add a secondary nameserver. Enter: • **Y** to enter a secondary nameserver. • **N** to proceed to the next step of the installation.
Another nameserver	IP address of the another DNS server you want to use if the primary server cannot be reached.
Primary NTP server	IP address or host name of the primary Network Time Protocol server you want to use (the default is **time.nist.gov**). The console will prompt you to add a secondary NTP server. Enter: • **Y** to enter a secondary NTP server. • **N** to proceed to the next step of the installation.
Another NTP servers	IP address of the another NTP server you want to use if the primary NTP server cannot be reached.
System Time Zone	The time zone you want to use.
Clock time	The clock time (based on the selected System Time Zone). This is the time that will be shown in the machine. Check that the time is correct based on your time zone and change it if necessary. See Time Zones SupportedCisco Evolved Programmable Network Manager. The console will prompt you to change the system clock time. Enter: • **Y** to change the clock time. • **N** to proceed to the next step of the installation.
Username	The name of the first administrative user (**admin** by default). This is the Cisco EPN Manager **CLI admin user** that logs into the Cisco EPN Manager server using SSH.
Password	The password for the first administrative user. The password must be at least 8 characters long, and must contain at least one number and one upper-case letter.

Note　　At the time of installation the user must use the IP subnet which is planned to be used for UI access. This IP will be configured on the eth0 interface known also as GigabitEthernet0 in admin CLI.

Step 3　　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 6.0 in a High Availability Deployment.

- Enter **no** if:
  - You are not using HA.
  - You are using HA but you want this server to be the primary server.

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

Step 5 Review your settings and:

- If the settings are correct, select **Y** to apply them.

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

Multi NIC Installation

These topics describe how to perform Multi NIC installation:

Note For multiple network adapter based systems (bare metal or virtual), ensure that at the time of installation, only a single adapter is enabled (one used for UI). Once EPNM is installed, power OFF the system, enable the additional network adapters and power it back ON.

You can also leave only the main interface (one used for UI) wired (connected), install EPNM, once it starts reconnect the adapters without rebooting the system.

Prerequisites

In an HA environment:

- Remove High Availability

- Add the configuration needed for the additional NIC

- Perform High Availability registration between Primary and Secondary Servers

Configure Additional NIC on Primary and Secondary Servers

Enter these commands in the admin CLI.

```
storm-ha-194/admin# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
storm-ha-194/admin(config)# interface GigabitEthernet 1
```

```
storm-ha-194/admin(config-GigabitEthernet)# ip address 172.23.222.32 255.255.255.0
Changing the hostname or IP may result in undesired side effects,
such as installed application(s) being restarted.
Are you sure you want to proceed? [y/n] y
storm-ha-194/admin(config-GigabitEthernet)# end
```

Note This configuration should be applied on both the servers (primary and secondary).

Add Static Route for Device Subnets in Primary and Secondary server

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

Operation of a Multi-NIC Server

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

In a HA environment:

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

- Depending on the configuration, failure of additional NIC will trigger Failover. For more details, please see Enable Multi NIC Monitoring

Remove IP Configuration

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

Enable Multi NIC Monitoring

Cisco EPN Manager allows you to add multiple interfaces that can be monitored. Upon registration the configuration of the monitored NICs will be copied into the secondary server and starting this point, the system will monitor the interfaces. If the primary server's monitored interfaces go down, the system will perform failover into the secondary server(only if all monitored interfaces are up and running on the secondary server). In case of failback to a new primary server, monitored NICs will be copied to the new primary server. If the primary server and the secondary server have different amount of enabled NICs, registration and failback to fresh primary operations will be prohibited (the system will notify with proper message).

To enable multiple NIC (monitoring) support:

- Log into the server as the Cisco EPN Manager CLI admin user.

- Enter the following command to add an interface:

```
ncs ha monitor interface add <interface-name>
```

> **Note** To delete an interface, enter the following command:
>
> ```
> ncs ha monitor interface del <interface-name>
> ```

- (Optional) Verify the configuration by running the following command:

  ```
  show run
  ```

Uninstall Cisco EPN Manager

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

Uninstall Cisco EPN Manager (OVA/VM)

Before You Begin

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

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

Step 2 Power off the virtual machine.

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

Uninstall Cisco EPN Manager (ISO/Bare Metal)

Before You Begin

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

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

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