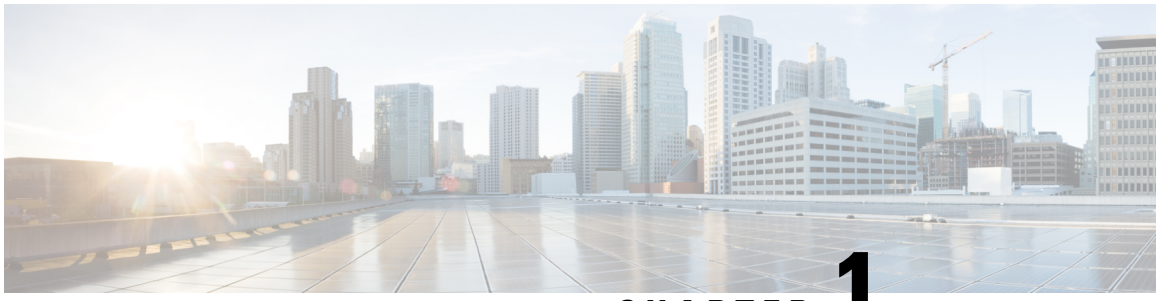
Installation Guide for Cisco Evolved Programmable Network Manager 7.0

First Published: 2023-01-28

Last Modified: 2023-01-28

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



CHAPTER 1

Cisco EPN Manager 7.0 Installation

This chapter provides the information required for planning your installation of Cisco EPN Manager 7.0 and ensuring that you meet all the prerequisites required for the installation. It also provides procedures for installing Cisco EPN Manager 7.0 in a standard, non-high availability environment. For high availability, see Cisco EPN Manager 7.0 High Availability Installation, on page 19.

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 7.0 can be installed as a fresh installation on a virtual machine. If you are already using a previous version of Cisco EPN Manager, you can upgrade to Cisco EPN Manager 7.0 and thereby retain your data.

The following topics provide an overview of the Cisco EPN Manager 7.0 installation and upgrade options and provide additional useful installation-related information.

- Installation Options
- Upgrade Options
- 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 7.0 on a virtual machine (VM):

- 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.

Note For Cisco EPN Manager 7.0 installation on 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 To install Cisco EPN Manager on non-Cisco hardware, use VMware and install the OVA file. Using VMware will minimize hardware non-compliance issues, however, you must make sure that your hardware has the resources required to allow provisioning of the VM.

OVA installation includes 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 7.0 by following the valid upgrade path relevant for your existing deployment. See Valid Upgrade Paths, on page 27.

The following methods are available for upgrading to Cisco EPN Manager 7.0:

- 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 (No HA).

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 7.0:

Hardware and Software Requirements

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 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
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

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

- 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 browser).

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.

Port	Protocol	Usage	Safe to Disable?	Notes
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	—
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 HA configured)	—
8087	TCP	To update software on the HA secondary backup server (uses HTTPS as transport).	No	—
9991	UDP	To receive Netflow data packets.	Yes	Cisco EPN Manager does not support Netflow. You should disable this traffic in the network firewall.
9992	TCP	To manage M-Lync using HTTP or HTTPS.	Yes	Cisco EPN Manager does not support M-Lync. You should disable this traffic in the network firewall.

Port	Protocol	Usage	Safe to Disable?	Notes
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**

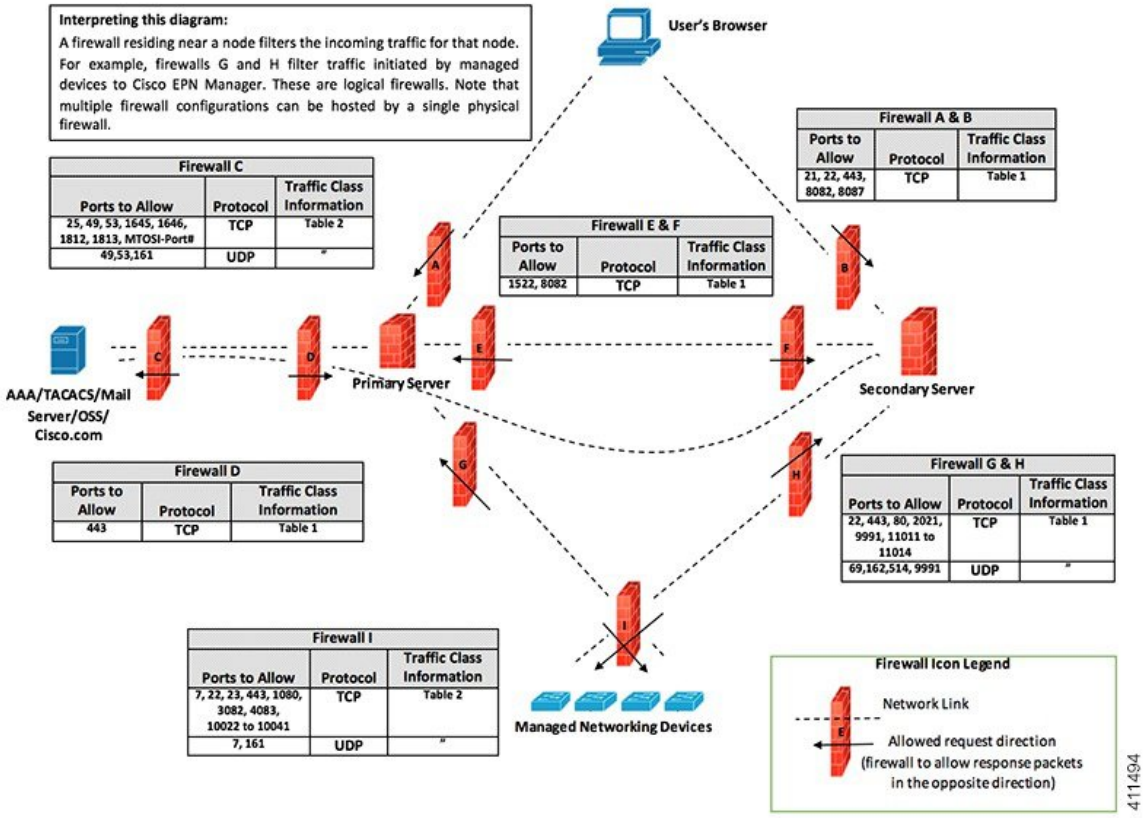
The following table lists the destination ports on external devices that may be protected by a firewall. These ports are used by Cisco EPN Manager to connect to network devices. You must open the required ports to allow Cisco EPN Manager to connect to these devices.

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.
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.

Port	Protocol	Used to:
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.

Do not make copies of licenses.

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

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

Prerequisites for OVA/VM Installations

Before installing Cisco EPN Manager, 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 OVA Package.

Verify the OVA Package

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

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.

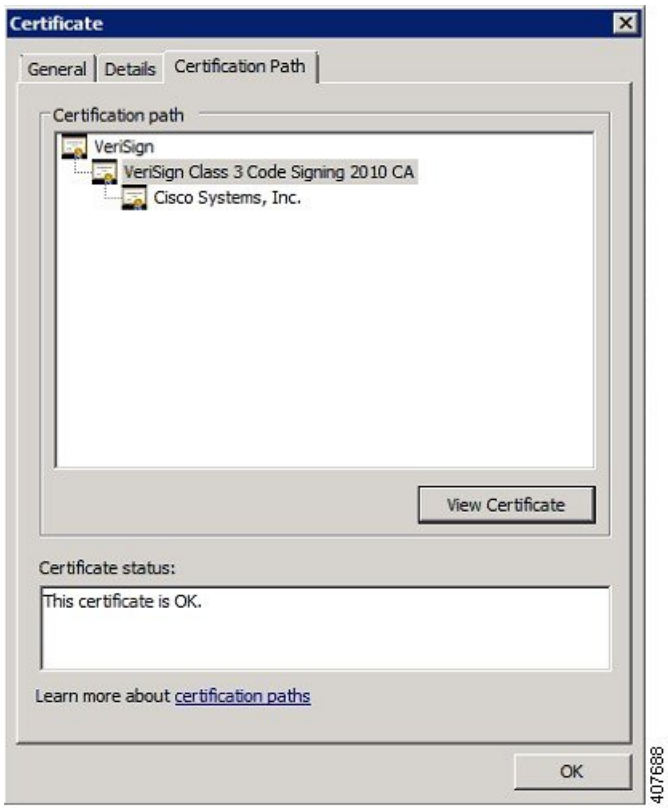
   Note Do not validate the image using the information in the Vendor field. This field does not authenticate Cisco Systems as the publisher.

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.



Install Cisco EPN Manager 7.0 (No HA)

Install Cisco EPN Manager Using an OVA/VM

1. Make sure your deployment meets the requirements in System Requirements.
2. Make sure your deployment meets the prerequisites in Prerequisites for OVA/VM Installations. This includes verifying the OVA package.
3. Deploy the OVA from the VMware vSphere Client.
4. Set the System Time of the Deployed OVA
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.

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.

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.
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. 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 7.0 in a High Availability Deployment, on page 23.
- 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, 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)

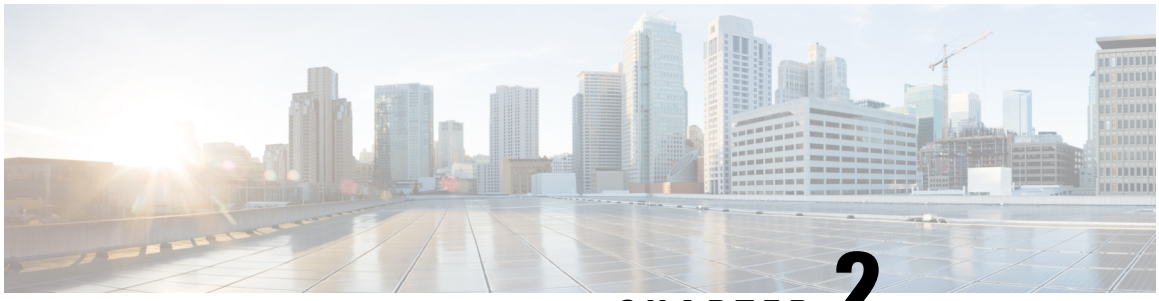
Before You Begin

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.



CHAPTER 2

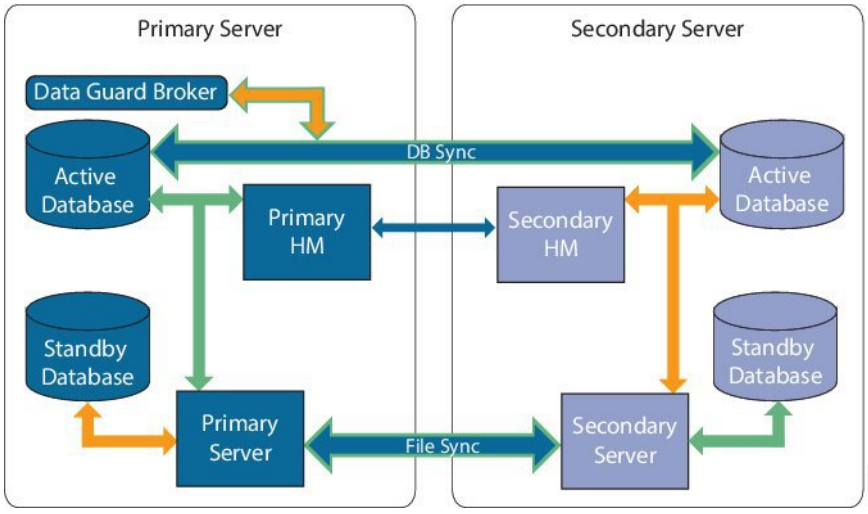
Cisco EPN Manager 7.0 High Availability Installation

This chapter provides information about Cisco EPN Manager in a high availability environment:

High Availability Overview

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

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



A high availability deployment consists of a primary and a secondary server with Health Monitor (HM) instances (running as application processes) on both servers. When the primary server fails (due to a problem

or because it is manually stopped), the secondary server takes over and manages the network while you restore access to the primary server. If the deployment is configured for automatic failover, the secondary server takes over the active role within two to three minutes after the primary server failure.

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

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

High Availability Deployment Considerations

High Availability Deployment Models

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

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

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

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

events to that single virtual IP address. Without a virtual IP address, you must configure your devices to forward events to both the primary and secondary servers.

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

Understand High Availability Limitations

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

- The HA system requires a minimum of 500 Mbps (Mega bit per second) or higher of network bandwidth 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 HA system requires low latency (maximum 100 ms, preferably under 70 ms.) across network links between the primary and secondary servers. Irrespective of the physical proximity of these two servers, high latency on these links can affect how Cisco EPN Manager maintains sessions between the primary and secondary servers. This is because larger databases require more synchronization transactions which require lower latency and higher bandwidth. If you are managing a relatively small network using Cisco EPN Manager, your database would be smaller and therefore, HA might work with a higher network latency and less bandwidth.
- HA performance is always sensitive to the network throughput delivered by the network that connects the primary and secondary servers. This restriction applies (to some degree) to all of the deployment models. For example, in a geographically dispersed deployment, a Remote HA deployment is more likely to have problems due to low bandwidth and high latency. However, if Local and Campus HA deployments are not properly configured, they are highly susceptible to problems with latency that result from bandwidth limitations on high-usage networks.

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

Consider Whether You Can Use Virtual Addresses

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

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

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

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

- Subnet mask: 255.255.255.224 (/27)
- Primary server IP address: 10.10.101.1
- Secondary server IP address: 10.10.101.2
- Virtual IP address: 10.10.101.[3-30] e.g., 10.10.101.3. Note that the virtual IP address can be any of a range of addresses that are valid for the given subnet mask.

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

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

Prerequisites for High Availability Installations

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

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

is, when you register the secondary server on the primary server (also called *pairing* the servers). Finally, you will need it to log in to the secondary server's Health Monitor page.

- A Cisco EPN Manager web GUI user ID with Administration privileges on the primary server. You will also need the user's password.
- A valid email address to which HA notifications can be sent.

Install Cisco EPN Manager 7.0 in a High Availability Deployment

The procedure in this section is for a fresh installation of the product in a high availability environment. If you are upgrading to Cisco EPN Manager 7.0 from a previous version, see Upgrade to Cisco EPN Manager 7.0 (High Availability).

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 7.0 (No HA).

Step 2 Install Cisco EPN Manager on the secondary server as described in Install Cisco EPN Manager 7.0 (No HA).

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. (During normal operation, you will need to enter the HA authentication key to log in to the secondary server's Health Monitor page.)

Step 5 Enter the password again to confirm.

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

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

Step 8 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 9 Configure HA by registering the secondary server on the primary server. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server, in the Cisco Evolved Programmable Network Manager User and Administrator Guide .

Check Readiness for HA Configuration

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

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

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

If the primary and secondary authentication keys are different, then Check Readiness shall not proceed. You can proceed with HA Registration.

To check readiness for HA configuration, follow these steps:

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

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

Step 3 Select **HA Configuration**.

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

Step 5 Click **Check Readiness**.

A pop-up window with the system specifications and other parameters will be displayed. The screen will show the checklist item name, status, impact, and recommendation details.

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

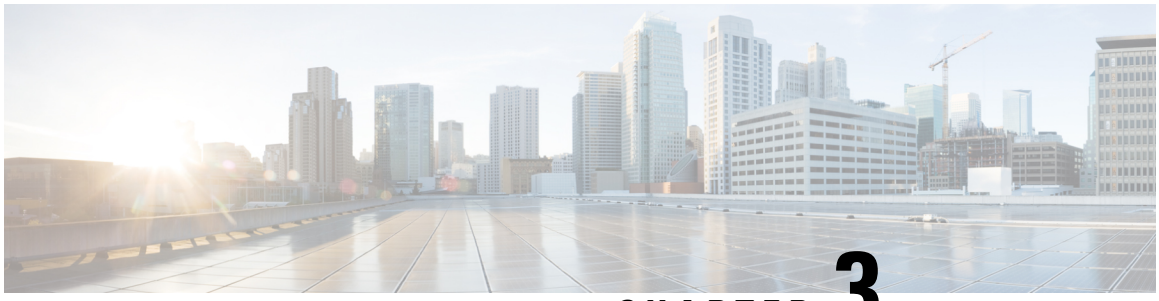
Table 3: Checklist name and description

Checklist Test Name	Test Description
SYSTEM - CHECK CPU COUNT	Checks the CPU count in the primary and secondary servers. The CPU count in both servers must satisfy the requirements.
SYSTEM - CHECK DISK IOPS	Checks the disk speed in the primary and secondary servers. The minimum expected disk speed is 200 MBps.
SYSTEM - CHECK RAM SIZE	Checks the RAM size of the primary and secondary servers. The RAM size of both servers must satisfy the requirements.
SYSTEM - CHECK DISK SIZE	Checks the disk size of the primary and secondary servers. The disk size of both servers must satisfy the requirements.
SYSTEM - CHECK SERVER PING REACHABILITY	Checks that the primary server can reach the secondary server through a ping.
SYSTEM - CHECK OS COMPATABILITY	Checks that the primary server and secondary servers have the same OS version.

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

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

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



CHAPTER 3

Upgrade to Cisco EPN Manager 7.0

You can upgrade to Cisco EPN Manager 7.0 by following one of the Valid Upgrade Paths, on page 27.

This chapter provides instructions for upgrading to Cisco EPN Manager 7.0 using Backup-restore upgrade.

Backup-restore upgrade —Involves backing up all data from the currently installed version of Cisco EPN Manager, then installing Cisco EPN Manager 7.0 on a new server, then restoring the backed up data to the new Cisco EPN Manager 7.0 server.

Valid Upgrade Paths

The following table lists the valid paths for installing/upgrading to Cisco EPN Manager 7.0 from previous versions.

Current Cisco EPN Manager Version	Installation Path to Cisco EPN Manager 7.0.0
Cisco EPN Manager 6.0.2	**Cisco EPN Manager 6.0.2 > 7.0.0**
Cisco EPN Manager 6.1.1	**Cisco EPN Manager 6.1.1 > 7.0.0**

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

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

Prerequisites for Upgrading to Cisco EPN Manager 7.0

Before starting the upgrade:

1. Ensure that you have followed the relevant upgrade path based on your current version of Cisco EPN Manager. See Valid Upgrade Paths, on page 27.
2. Ensure that your deployment meets the requirements in the relevant prerequisites topic:
   - Prerequisites for OVA/VM Installations. For OVA/VM deployments, the upgrade is run from the vmWare vSphere client.
3. Remove any devices running uncertified software versions from Cisco EPN Manager. This step is not mandatory but highly recommended.
4. Back up your data. See Create a Copy of Your Data.
5. Ensure that no backups are running.
6. Ensure that SCP is enabled on your client machine and the required ports are open (see Ports Used by Cisco EPN Manager). You will need to use SCP to copy files from your client machine to the Cisco EPN Manager server.
7. Copy any gpg files located in /localdisk/defaultRepo to an external repository and then delete them from this folder.

Note Customers using OTDR feature for NCS1001 in EPNM, must perform the following:

```
Take a backup of /opt/CSCOlumos/conf/ncs1k-otdr-ports.xml. The below feature entry has to
be updated in /opt/CSCOlumos/conf/Migration.xml to retain the OTDR mapping configuration
done for NCS1001 devices.
<feature name="Otdr-ports-Properties">
<files>
<file optional="true">/opt/CSCOlumos/conf/ncs1k-otdr-ports.xml</file>
</files>
</feature>
```

Create a Copy of Your Data

To create a copy of your current data, backup your data to a remote repository. Refer to the backup topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide . If necessary, you can revert to the previous version by restoring the data. See Revert to the Previous Version using Data Restore.

Upgrade to Cisco EPN Manager 7.0 (No HA)

These topics explain how to upgrade to Cisco EPN Manager 7.0 from an earlier version of Cisco EPN Manager in a standard deployment (no high availability).

- Backup-Restore Upgrade (No HA)
- Post-Upgrade Tasks

If you are performing an upgrade in a high availability deployment, see Upgrade to Cisco EPN Manager 7.0 (High Availability), on page 30.

Backup-Restore Upgrade (No HA)

Backup-restore upgrade involves backing up all data from the currently installed version of Cisco EPN Manager, then installing Cisco EPN Manager 7.0 on a new server, then restoring the backed up data to the new Cisco EPN Manager 7.0 server. This is the recommended upgrade method.

Before You Begin

- Make sure the new server has the same hardware specifications as the server from which the backup was taken.
- Note the location of the remote backup repository used by the old server. You will need it to configure the same backup location on the new server.

Step 1 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 2 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 .

Post-Upgrade Tasks

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

New dashlets on existing tabs, will not be added automatically post upgrade. The user can manually add them from the dashboard menu Settings->Add Dashlet(s).

Manually created command sets (for example: ip access-list, Team Interface or interface GigabitEthernet 1, additional ntp servers and ip route) will not be available post upgrade. The user needs to add them manually. Refer to the **Command Reference Guide for Cisco Evolved Programmable Network Manager**

New dashboard tabs will be added automatically.

Upgrade to Cisco EPN Manager 7.0 (High Availability)

The following topic provides the procedure for upgrading to Cisco EPN Manager 7.0 in a high availability deployment:

Backup-Restore Upgrade (High Availability)

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

Backup-Restore Upgrade (High Availability)

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

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

Before You Begin

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

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

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

b. Choose **Administration > Settings > High Availability**.

c. Make a 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 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 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 4 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 5 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. Ensure that, at a minimum, the following services are up and running: Health Monitor, Database, NMS, SAM Daemon, DA Daemon, Compliance Engine. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

Step 6 Once the restore is completed, perform the post-upgrade tasks on the primary server. See Post-Upgrade Tasks.

Step 7 Re-configure HA by registering the secondary server on the primary server. Use the information you saved in *Step 1*. The registration process must be performed from the primary server. For more information, see the section on registering the secondary server on the primary server, in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

Post-Upgrade Tasks

- If you are using Cisco Smart Licensing, re-register Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. Refer to the topics that describe managing licenses in the Cisco Evolved Programmable Network Manager User and Administrator Guide .
- Synchronize the inventory of all devices with the database, as follows:
  1. In the Cisco EPN Manager GUI, choose **Monitor > Network Devices**.
  2. Select all devices, then click **Sync**.
- Instruct users to clear the browser cache on all client machines that accessed an older version of Cisco EPN Manager before they try to connect to the upgraded Cisco EPN Manager server.
- If you were using external AAA before the upgrade, configure external authentication again. Refer to the user management topics in the Cisco Evolved Programmable Network Manager User and Administrator Guide.

- During the upgrade, the Cisco EPN Manager home page will be reset to the default home page (Getting Started page). Users can select their own default home page from the Getting Started page or from the Settings menu at the top right of the page.

New dashlets on existing tabs, will not be added automatically post upgrade. The user can manually add them from the dashboard menu Settings->Add Dashlet(s).

Manually created command sets (for example: ip access-list, Team Interface or interface GigabitEthernet 1, additional ntp servers and ip route) will not be available post upgrade. The user needs to add them manually. Refer to the **Command Reference Guide for Cisco Evolved Programmable Network Manager**

New dashboard tabs will be added automatically.

Revert to the Previous Version of Cisco EPN Manager

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

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

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

- If you used the backup facility, see Revert to the Previous Version using Data Restore.
- If you took a VM snapshot, see Revert to the Previous Version Using the VM Snapshot.

Revert to the Previous Version using Data Restore

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

For non-HA environments, do the following:

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

For HA environments, do the following:

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

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

Revert to the Previous Version Using the VM Snapshot

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

For non-HA environments, do the following:

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

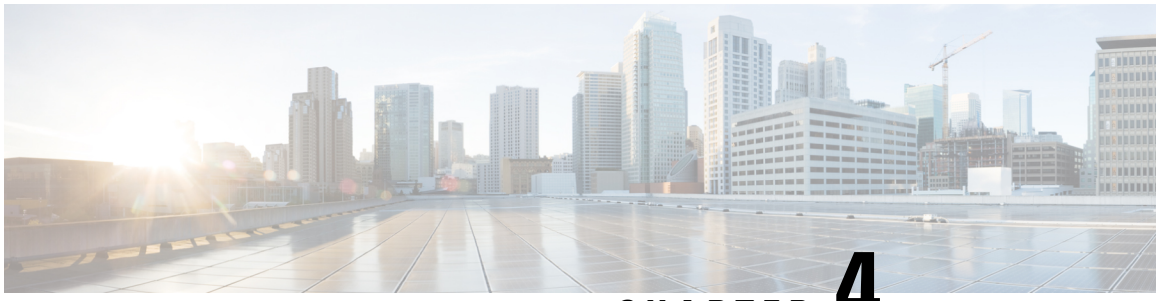
```
ncs start
```

For HA environments, do the following:

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

```
ncs start
```

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



CHAPTER 4

Install Geo Map Resource Files for Offline Use

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

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

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

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

Install Geo Map Resource Files (Standard Deployment)

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

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

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

Before You Begin

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

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

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

a. Go to the Software Download site on Cisco.com .
b. Navigate to the files by choosing **All Releases >7.0**.
c. Identify the map you want to download and click **Download**.
d. Follow the instructions to save the file to the client machine.

Step 2 Copy the geo map compressed files from the local machine to the Cisco EPN Manager server's default local repository (/localdisk/defaultRepo).

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

```
scp joesmith@123.456.789.101:/temp/Russia_GeoMap_CEPNM_7_0_0-bundle.tar.gz/localdisk/defaultRepo
```

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

Before You Begin

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

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

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

Example:

```
application install filename defaultRepo
```

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

Example:

```
application install Russia_GeoMap_CEPNM_5_0_0-bundle.tar.gz defaultRepo
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes
Please ensure you have a backup of the system before proceeding.Proceed with the application install
 ? (yes/no) [yes] ? yes
```

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

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

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

Step 2 Check **Enable Geo Maps**.

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

Step 4 Click **Save**.

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

Verify that the Geo Maps Files Were Installed Successfully

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

Check that the map is being displayed in the GUI:

a. Log in to the Cisco EPN Manager web GUI as a user with Administrator privileges.

b. From the left sidebar menu, choose **Maps** > **Topology Maps** > **Network Topology**.

c. Click the Geographical Map icon at the top right of the topology window to display the geo map.

d. Verify that the desired map is displayed.

Install Geo Map Resource Files (High Availability Deployment)

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

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

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

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

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

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

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

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

Update Geo Map Resource Files After Upgrading to Cisco EPN Manager

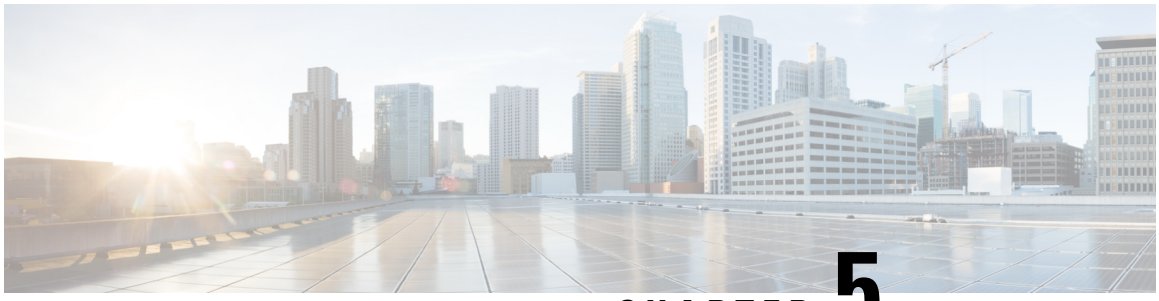
Geo map files must be reinstalled after upgrade.

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

Step 2 Stop and restart the server(s).

Step 3 Clear the cache.

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



CHAPTER 5

Supplementary Installation-Related Information and Procedures

Log Into the Cisco EPN Manager Web GUI

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

Step 1 On a client machine, launch one of the supported browsers.

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

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

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

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

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

Step 5 For increased security, perform these steps:

a. Change the password for the web GUI root user by choosing **Administration** > **Users** > **Roles & AAA** > **Change Password**.

b. 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 .

c. 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 .