Cisco EPN Manager 4.1 Installation

This chapter provides the information required for planning your installation of Cisco EPN Manager 4.1 and ensuring that you meet all the prerequisites required for the installation. It also provides procedures for installing Cisco EPN Manager 4.1 in a standard, non-high availability environment. For high availability, see Cisco EPN Manager 4.1 High Availability.

Installation Overview

Cisco EPN Manager 4.1 can be installed as a fresh installation by following the given steps:

1. Install Cisco EPN Manager 4.0 either on a virtual machine or a bare metal server.

   You can refer to Cisco EPN Manager 4.0 Installation Guide

2. Install Cisco EPN Manager 4.1 UBF as explained in the steps in this guide

The following topics provide information and procedures for installing Cisco EPN Manager 4.1 UBF in standard and high availability deployments.

Note Before starting the installation procedure, please review the release notes for important information or issues relating to the installation.

Installation Paths for Cisco EPN Manager 4.1

The following table lists the valid paths for installing Cisco EPN Manager 3.1 from previous versions.

Current Cisco EPN Manager Version	Installation Path to Cisco EPN Manager 4.1
Cisco EPN Manager 4.0	**Cisco EPN Manager 4.0 > 4.1**
Cisco EPN Manager 4.0.1	**Cisco EPN Manager 4.0.1 > 4.1**
Cisco EPN Manager 4.0.2	**Cisco EPN Manager 4.0.2 > 4.1**

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

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

Prerequisites for Cisco EPN Manager 4.1 Installation

Note Cisco EPN Manager 4.1 installation consists of Cisco EPN Manager 4.0 OVA/ISO installation followed by Cisco EPN Manager 4.1 UBF installation.

Before installing Cisco EPN Manager 4.1, you must perform the following tasks:

- Ensure that you have installed Cisco EPN Manager 4.0 either on a virtual machine or a bare metal server.

  You can refer to Cisco EPN Manager 4.0 Installation Guide:

- Licensing, on page 2
- Disable Automatic Client Logout

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.

Disable Automatic Client Logout

If the client is inactive for a certain period of time, you might be automatically logged out. To avoid being logged out during the installation, we recommend that you disable automatic logout of idle users in the system settings, as follows:

Step 1 Go to **Administration** > **Settings** > **System Settings** > **Server**.

Step 2 In the Global Idle Timeout section, uncheck the **Logout all idle users** check box.

Step 3 Click **OK** in the displayed message reminding you to save your change to the system settings.

Step 4 Click **Save**.

Step 5 Click the **gear icon** at the top right of the web GUI window, then click **My Preferences**. Under User Idle Timeout, uncheck the **Logout idle user** check box.

Step 6 Click **Save**.

Step 7 Log out and then log back into Cisco EPN Manager.

Install Cisco EPN Manager 4.1 in a Standard Environment (No HA)

Follow these steps to install Cisco EPN Manager 4.1 in a standard environment (no high availability).

1. Make sure you have performed the tasks in Prerequisites for Cisco EPN Manager 4.1 Installation.
2. Place the Cisco EPN Manager 4.1 Installation File on the Server.
3. Install Cisco EPN Manager 4.1 (No HA).
4. Perform an inventory collection for all devices to synchronize them with the database. See Synchronize the Inventory of All Devices with the Database (Existing Deployments Only).

If you are using external authentication and authorization, after installation you must export the user task information to your AAA server in order to pick up the latest updates. See the Cisco Evolved Programmable Network Manager User and Administrator Guide for more information.

Place the Cisco EPN Manager 4.1 Installation File on the Server

This procedure explains how to download the ubf installation file to your local machine, then upload it from your local machine to the Cisco EPN Manager server.

Note You need an account on Cisco.com in order to download the installation file.

Step 1 Make sure you have performed the tasks in Prerequisites for Cisco EPN Manager 4.1 Installation.

Step 2 Download the required ubf file to your local machine.

a. Go to the Software Download site on Cisco.com.

b. Locate the Cisco EPN Manager Minor Release file (in the format **cepn4.1-buildXXX.ubf**).

c. Download the file to your local machine.

Step 3 After the file is downloaded to the local server, make sure to compare the checksum (MD5) with the one available on Cisco.com.

Step 4 Log into the Cisco EPN Manager web GUI as a user with Administrator privileges.

Step 5 Upload the ubf file from your local machine to the Cisco EPN Manager server.

a. From the left sidebar menu, choose **Administration > Software Update**.

b. Click the blue **Upload** link at the top of the page

.

c. In the Upload Update dialog box, click **Browse** and navigate to the file you downloaded previously.

d. Click **OK** to upload the file to the server.

After the successful upload of Cisco EPN Manager 4.1, the software will appear under the Files tab.

Install Cisco EPN Manager 4.1 (No HA)

Follow this procedure to install Cisco EPN Manager 4.1 in a standard environment with no high availability.

Step 1 From the left sidebar, choose **Administration** > **Software Update**.

Step 2 Click the **Install** button associated with EPN Manager 4.1 on the Software Update page.

Step 3 Click **Yes** in the confirmation message pop-up window to proceed with the installation.

Note The server will restart when the installation is complete.

Step 4 If you are asked whether to overwrite an existing file, click **Yes**.

After successful installation, the status will change to **Installed**. Cisco EPN Manager will auto-restart and the Cisco EPN Manager web GUI will not be accessible for some time.

Step 5 Check the status of the Cisco EPN Manager services.

a. Start an SSH session with the Cisco EPN Manager server and log in as the Cisco EPN Manager CLI admin user.
b. Run the **ncs status** command to 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 When the Cisco EPN Manager web GUI is accessible, log in and check that the Cisco EPN Manager Minor Release's status is “Installed” in the Software Update page.

a. From the left sidebar, choose **Administration** > **Software Update**.
b. Verify that **Cisco EPN Manager Minor Release** is listed as Installed under the Updates tab. Also verify that the ubf file (in the format **cepnm4.1-buildXXX.ubf**) is listed in the Files tab and that the In Use status is **Yes**.

What to do next

Note The service restart in the Synchorization Clock operation can be ignored as the installation of Cisco EPN Manager Minor Release restarts the Cisco EPN Manager.

Synchronize the Inventory of All Devices with the Database (Existing Deployments Only)

If you have already been using a previous version of Cisco EPN Manager (i.e., this is not a fresh installation), you need to perform a Sync operation on the devices. The Sync operation instructs Cisco EPN Manager to collect device physical and logical inventory and save the information to the database.

Step 1 Choose **Monitor** > **Network Devices**.
Step 2 Select all devices, then click **Sync**.

Install Cisco EPN Manager 4.1 in a High Availability Environment

Follow these steps to install Cisco EPN Manager 4.1 in a HA environment.

1. Perform the General and HA Installation Prerequisite Tasks.
2. Remove the HA Configuration.
3. Place the Cisco EPN Manager 4.1 Installation File on the Server (HA Deployment).
4. Install Cisco EPN Manager 4.1 on Primary and Secondary Servers (HA Deployment).
5. Synchronize the Inventory of All Devices with the Database (Existing Deployments Only).

Note If you are using external authentication and authorization, after installation you must export the user task information to your AAA server in order to pick up the latest updates.

Perform the General and HA Installation Prerequisite Tasks

Before starting the HA installation, do the following:

1. Perform the tasks in Prerequisites for Cisco EPN Manager 4.1 Installation on both primary and secondary servers.

Remove the HA Configuration

Note This process is required only if the servers are associated with HA configuration.

Step 1 Make sure you have performed the tasks in Prerequisites for Cisco EPN Manager 4.1 Installation.

Step 2 Log into the Cisco EPN Manager web GUI on the primary server as a user with Administrator privileges.

Step 3 From the left sidebar, choose **Administration** > **Settings** > **High Availability**.

Step 4 Click **HA Configuration** on the left.

Step 5 Click **Remove**.

Step 6 When the remove operation completes, confirm that the Configuration Mode field displays **HA Not Configured**.

Place the Cisco EPN Manager 4.1 Installation File on the Server (HA Deployment)

Before You Begin

Make sure you have the password (authentication key) that was created when HA was enabled. You will need it to install the patch on the secondary server.

Step 1 Make sure you have removed the HA configuration as described in Remove the HA Configuration.

Step 2 On the primary server, upload the Cisco EPN Manager 4.1 ubf file. Follow the procedure in Place the Cisco EPN Manager 4.1 Installation File on the Server.

Step 3 Upload the Cisco EPN Manager 4.1 ubf file to the secondary server. (You will use the same file that was uploaded and installed on the primary server.)

a. Log into the secondary server's HM web page by entering the following URL in your browser:

`https://`*serverIP*`:8082`

Where *serverIP* is the IP address or host name of the secondary server.

a. Enter the authentication key and click **Login**.
b. Click **Software Update** at the top right of the Health Monitor window to open the Secondary Server Software Update window.
c. Enter the authentication key and click **Login**.
d. Click the **Upload** link under the window title, browse to the ubf file, and click **OK**.

After the successful upload of the ubf file, the file will appear under the Files tab.

What to do next

Install Cisco EPN Manager 4.1 on Primary and Secondary Servers (HA Deployment).

Install Cisco EPN Manager 4.1 on Primary and Secondary Servers (HA Deployment)

Before You Begin

- Make sure you have the password (authentication key) that was created when HA was enabled. You will need it to install the Cisco EPN Manager Minor Release file on the secondary server.
- Make sure no backups are in progress.

This ensures that the compliance server will be up and running on the secondary server after failover.

Step 1 Install Cisco EPN Manager 4.1 on the primary server and verify the installation, as described in Install Cisco EPN Manager 4.1 (No HA). After the installation, the primary server automatically restarts and the web GUI will not be accessible for some time.

Step 2 Synchronize the hardware and NTP clocks on both the primary and secondary servers, then check that the clocks on each server are synchronized with one another.

Note The service restart in the Synchorization Clock operation can be ignored as the installation of Cisco EPN Manager Minor Release restarts the Cisco EPN Manager.

Step 3 Install Cisco EPN Manager 4.1 on the secondary server.

a. Log into the secondary server's HM web page by entering the following URL in your browser:
`https://`*serverIP*`:8082`

   Where *serverIP* is the IP address or host name of the secondary server.

b. Enter the authentication key and click **Login**.
c. Click **Software Update** at the top right of the Health Monitor window to open the Secondary Server Software Update window.
d. Enter the authentication key and click **Login**.
e. Click the **Install** button associated with Cisco EPN Manager Minor Release on the Software Update page.
f. Click **Yes** in the confirmation message pop-up window to proceed with the installation. On successful installation, the status will change to **Installed** and the secondary server will restart automatically.

Step 4 After the secondary server has restarted, verify the installation on the secondary server.

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

b. Run the **ncs status** command to 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.

c. Once the web GUI is accessible, verify the installation and version in the secondary server's HM web page. Enter the following URL in your browser: **`https://`***serverIP*`:8082`

Where **`serverIP`** is the IP address or host name of the secondary server.

d. Enter the authentication key and click **Login** .

e. Click **Software Update** at the top right of the Health Monitor window to open the Secondary Server Software Update window.

f. Enter the authentication key and click **Login** .

g. In the Files tab, verify that the Cisco EPN Manager Minor Release file (in the format **cepnm4.1-buildXXX.ubf**) is listed and that the In Use status is **Yes**.

Step 5 Ensure that all services are up and running by running this command:

```
ncs status
```

Step 6 On the primary server, enable high availability and verify that the primary server's HA status is Primary Active.

a. Enable high availability.

1. Log into the Cisco EPN Manager web GUI as a user with Administrator privileges.
2. From the left sidebar menu, choose **Administration > Settings > High Availability**.
3. Click **HA Configuration** on the left, then enter the secondary server's IP address, the secondary server's authentication key, and an email address to which Cisco EPN Manager should send HA state change notifications.
4. If you are using virtual IP addressing in your HA setup (if the primary and secondary servers are in the same subnet), check the Enable Virtual IP check box and enter the virtual IP address(es).
5. Check Readiness for HA by following the process mentioned in section Check Readiness for HA Configuration.
6. Click **Save**, then wait until the servers are synchronized.
7. Verify that the Configuration Mode is **HA Enabled**.

b. Verify the primary server's HA status.

1. Click **HA Status** on the left.
2. Check that the Current State Mode displays **Primary Active**.

Step 7 Verify that the secondary server's HA status is Secondary Syncing.

a. Log into the secondary server's HM web page by entering the following URL in your browser: **`https://`***serverIP*`:8082`

Where **`serverIP`** is the IP address or host name of the secondary server.

b. Enter the authentication key and click **Login** .

c. Verify that the Current State Mode is **Secondary Syncing** (with a green check mark).

Check Readiness for HA Configuration

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

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

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

To check readiness for HA configuration, follow these steps:

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

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

Step 3 Select **HA Configuration**.

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

Step 5 Click **Check Readiness**.

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

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

Table 1: Checklist name and description

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

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

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

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