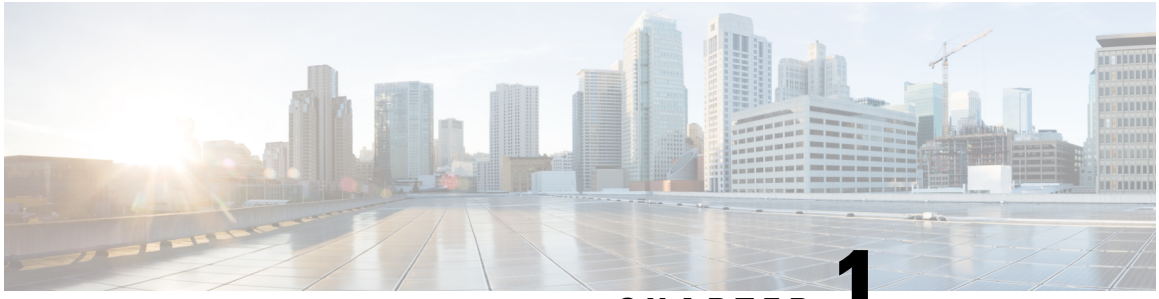
# Installation Guide for Cisco Evolved Programmable Network Manager 6.1

**First Published:** 2022-07-29

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

# CONTENTS



CHAPTER 1

# Cisco EPN Manager 6.1 Installation

This chapter provides the information required for planning your installation of Cisco EPN Manager 6.1 and ensuring that you meet all the prerequisites required for the installation. It also provides procedures for installing Cisco EPN Manager 6.1 in a standard, non-high availability environment. For high availability, see Cisco EPN Manager 6.1 High Availability Installation, on page 11.



## Installation Overview

Cisco EPN Manager 6.1 can be installed as a fresh installation by following the given steps:

1. Install Cisco EPN Manager 6.0 either on a virtual machine.

   You can refer to Installation Guide for Cisco Evolved Programmable Network Manager 6.0

2. Install Cisco EPN Manager 6.1 UBF as explained in the steps in this guide

The following topics provide information and procedures for installing Cisco EPN Manager 6.1 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.

# Upgrade Paths for Cisco EPN Manager 6.1

The following table lists the valid paths for upgrading to Cisco EPN Manager 6.1 from previous versions.

| Current Cisco EPN Manager Version | Installation Path to Cisco EPN Manager 6.1.0 |
|---|---|
| Cisco EPN Manager 6.0.0<br>Cisco EPN Manager 6.0.1 | **Cisco EPN Manager 6.0.0 (restore) > 6.0.1 > 6.1.0** |
| Cisco EPN Manager 6.0.2 | **Cisco EPN Manager 6.0.0 (restore) > 6.0.2 > 6.1.0** |
| Cisco EPN Manager 5.1.4.1 | **Cisco EPN Manager 5.1.4.1 > 6.0.0 (restore) > 6.0.1 > 6.1.0** |

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 Cisco EPN Manager 6.1 Installation

**Note** Cisco EPN Manager 6.1 installation consists of Cisco EPN Manager 6.0 OVA installation followed by Cisco EPN Manager 6.1 UBF installation.

Before installing Cisco EPN Manager 6.1, you must perform the following tasks:

- Ensure that you have installed Cisco EPN Manager 6.0 either on a virtual machine.

  You can refer to Installation Guide for Cisco Evolved Programmable Network Manager 6.0:

- 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**, then select **General** > **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 6.1 in a Standard Environment (No HA)

Follow these steps to install Cisco EPN Manager 6.1 in a standard environment (no high availability).

1. Make sure you have performed the tasks in Prerequisites for Cisco EPN Manager 6.1 Installation.
2. Place the Cisco EPN Manager 6.1 Installation File on the Server.
3. Install Cisco EPN Manager 6.1 (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 6.1 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 6.1 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 **cepn6.1-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 6.1, the software will appear under the Files tab.

# Install Cisco EPN Manager 6.1 (No HA)

Follow this procedure to install Cisco EPN Manager 6.1 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 6.1 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. 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 **cepnm6.1-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 6.1 in a High Availability Environment

Follow these steps to install Cisco EPN Manager 6.1 in a HA environment.

1. Perform the General and HA Installation Prerequisite Tasks.
2. Remove the HA Configuration.
3. Place the Cisco EPN Manager 6.1 Installation File on the Server (HA Deployment).
4. Install Cisco EPN Manager 6.1 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:

- Perform the tasks in Prerequisites for Cisco EPN Manager 6.1 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** Log into the Cisco EPN Manager web GUI on the primary server as a user with Administrator privileges.

**Step 2** From the left sidebar, choose **Administration** > **Settings** > **High Availability**.

**Step 3** Click **HA Configuration** on the left.

**Step 4** Click **Remove**.

**Step 5** When the remove operation completes, confirm that the Configuration Mode field displays **HA Not Configured**.

# Place the Cisco EPN Manager 6.1 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 6.1 ubf file. Follow the procedure in Place the Cisco EPN Manager 6.1 Installation File on the Server.

**Step 3** Upload the Cisco EPN Manager 6.1 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.

**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 **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.

# Install Cisco EPN Manager 6.1 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 6.1 on the primary server and verify the installation, as described in Install Cisco EPN Manager 6.1 (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 6.1 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. 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 **cepnm6.1-buildXXX.ubf** ) is listed and that the In Use status is **Yes**.

**Step 5** 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 6** 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 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:

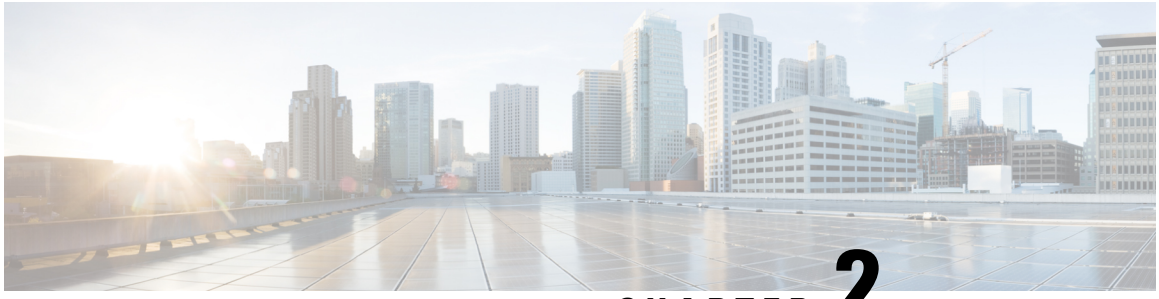
***Table 1: Checklist name and description***

| Checklist Test Name | Test Description |
|---|---|
| SYSTEM - CHECK CPU COUNT | Checks the CPU count in the primary and secondary servers.<br>The CPU count in both servers must satisfy the requirements. |
| SYSTEM - CHECK DISK IOPS | Checks the disk speed in the primary and secondary servers.<br>The minimum expected disk speed is 200 MBps. |
| SYSTEM - CHECK RAM SIZE | Checks the RAM size of the primary and secondary servers.<br>The RAM size of both servers must satisfy the requirements. |
| SYSTEM - CHECK DISK SIZE | Checks the disk size of the primary and secondary servers.<br>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 500 Mbps in primary and secondary servers.<br>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.<br>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.<br>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 2

# Cisco EPN Manager 6.1 High Availability Installation

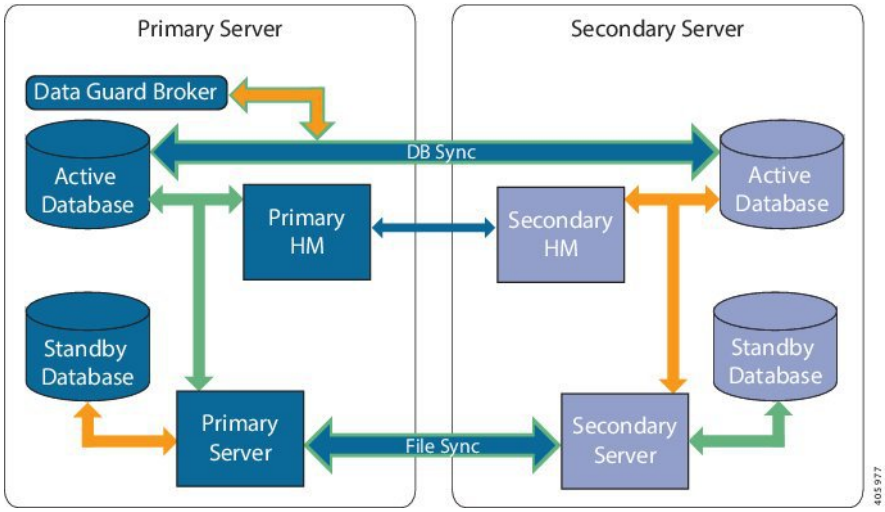
This chapter provides information about Cisco EPN Manager in a high availability environment:



## 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

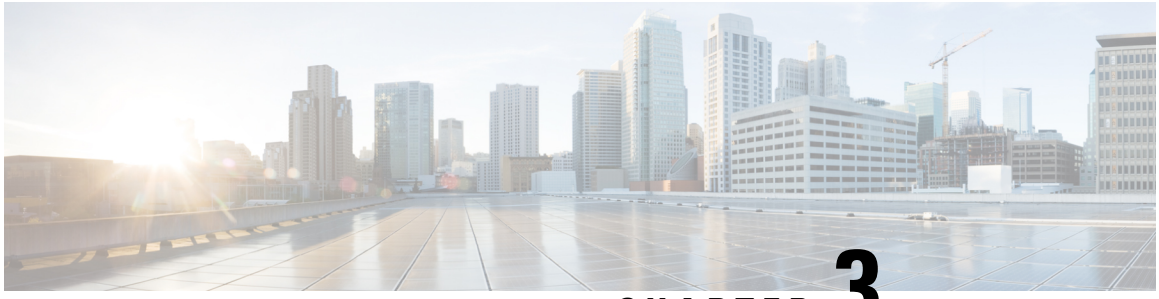
The following example illustrates how virtual, primary, and secondary IP addresses should be assigned with respect to each other. If the primary and secondary servers have the following IP address assignments within the given subnet, the virtual IP address for both servers can be assigned as follows:

- Subnet mask: 255.255.255.224 (/32)
- Primary server IP address: 10.10.101.1

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

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

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



CHAPTER 3

# Upgrade to Cisco EPN Manager 6.1

You can upgrade to Cisco EPN Manager 6.1 by following one of the Upgrade Paths for Cisco EPN Manager 6.1 , on page 2.

This chapter provides instructions for upgrading to Cisco EPN Manager 6.1 using Backup-restore upgrade.

**Note** Bare metal is not supported in Cisco EPN Manager 6.1. Migrate to ESXi based host before upgrading, if EPNM is not already running on virtual machine

Backup-restore upgrade consists of the following steps:

- Backup all data from the currently installed version of Cisco EPN Manager.
- Install Cisco EPN Manager 6.0 OVA (if current version is running on bera metal, you need to migrate to an ESXi based host first).
- Restore backup on the new Cisco EPN Manager 6.0.
- Install Cisco EPN Manager 6.1 UBF.



# Upgrade Paths for Cisco EPN Manager 6.1

The following table lists the valid paths for upgrading to Cisco EPN Manager 6.1 from previous versions.

| Current Cisco EPN Manager Version | Installation Path to Cisco EPN Manager 6.1.0 |
|---|---|
| Cisco EPN Manager 6.0.0<br>Cisco EPN Manager 6.0.1 | **Cisco EPN Manager 6.0.0 (restore) > 6.0.1 > 6.1.0** |
| Cisco EPN Manager 6.0.2 | **Cisco EPN Manager 6.0.0 (restore) > 6.0.2 > 6.1.0** |

| Current Cisco EPN Manager Version | Installation Path to Cisco EPN Manager 6.1.0 |
|---|---|
| Cisco EPN Manager 5.1.4.1 | **Cisco EPN Manager 5.1.4.1 > 6.0.0 (restore) > 6.0.1 > 6.1.0** |

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.

# Upgrade to Cisco EPN Manager 6.1 (No HA)

These topics explain how to upgrade to Cisco EPN Manager 6.1 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 6.1 (High Availability), on page 16.

## 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 6.1 on a new server, then restoring the backed up data to the new Cisco EPN Manager 6.1 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 .

# Upgrade to Cisco EPN Manager 6.1 (High Availability)

The following topic provides the procedure for upgrading to Cisco EPN Manager 6.1 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. Back up your data to a remote repository.
2. Perform a fresh installation of Cisco EPN Manager on both the primary and secondary servers.
3. Restore the backup data on the primary server.
4. 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 6.1 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** Backup 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. Note that for optimal Cisco EPN Manager functionality, all services should be up and running.

**Step 6** If the **ncs status** output on the primary server lists **Compliance engine is stopped**, do the following:

**a.** Stop Cisco EPN Manager.

```
ncs stop
```

**b.** Log in as the Linux CLI root user.

**c.** Update the time zone using a soft link (the following command is one line):

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

**Step 7** Once the restore is completed, perform the post-upgrade tasks on the primary server. See Post-Upgrade Tasks.

**Step 8** 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.

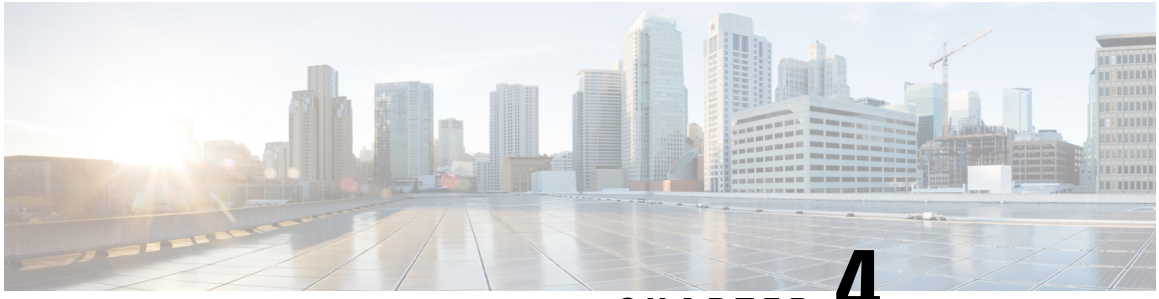
# Post-Upgrade Tasks

- 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).

New dashboard tabs will be added automatically.



CHAPTER 4

# Supplementary Installation-Related Information and Procedures



## Booting Into a Rescue Mode

**Step 1** Boot from Cisco EPN Manager ISO.

**Step 2** On the installation menu, choose **Cisco EPNM System Rescue Mode**.

**Step 3** When prompted about mounting the disks for the target system to be rescued, wait 20 seconds and select option 1 **Continue**. This will mount the system under /mnt/sysimage.when prompted to obtain a shell Press **Enter** . This shell will live inside the installation/rescue environment, with the target system mounted under /mnt/sysimage. This shell has a number of tools available for rescuing a system, such as all common file system, disk, LVM, and networking tools. The various bin directories of the target system are added to the default executable search path (${PATH}).

**Step 4** chroot into the /mnt/sysimage directory by running: chroot /mnt/sysimage

## Log Into the Cisco EPN Manager Web GUI

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

**Procedure**

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

**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 .

# Time Zones Supported

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

| | | |
|---|---|---|
| Africa/Abidjan | America/St_Johns | Europe/Amsterdam |
| Africa/Accra | America/St_Kitts | Europe/Belgrade |
| Africa/Addis_Ababa | America/St_Lucia | America/Los_Angeles |
| Africa/Algiers | America/St_Thomas | Europe/Bratislava |
| Africa/Asmara | America/St_Vincent | Europe/Brussels |
| Africa/Bamako | America/Swift_Current | Europe/Bucharest |
| America/Tegucigalpa | America/Thunder_Bay | Europe/Budapest |

| | | |
|---|---|---|
| Africa/Bangui | America/Tijuana | Europe/Chisinau |
| Africa/Banjul | America/Toronto | Europe/Copenhagen |
| Africa/Bissau | America/Vancouver | Europe/Dublin |
| Africa/Blantyre | America/Whitehorse | Europe/Gibraltar |
| America/Tortola | America/Winnipeg | Europe/Helsinki |
| Africa/Bujumbura | America/Yakutat | Europe/Isle_of_Man |
| Africa/Cairo | America/Yellowknife | Europe/Istanbul |
| Africa/Casablanca | Antarctica/Casey | Europe/Jersey |
| Africa/Ceuta | Antarctica/Davis | Europe/Kaliningrad |
| Africa/Conakry | Antarctica/DumontDUrville | Indian/Chagos |
| Africa/Dakar | Antarctica/Mawson | Indian/Christmas |
| Africa/Dar_es_Salaam | Antarctica/McMurdo | Indian/Comoro |
| Africa/Djibouti | Antarctica/Palmer | Asia/Jakarta |
| Africa/Douala | Antarctica/Rothera | Indian/Kerguelen |
| Africa/El_Aaiun | Antarctica/Syowa | Indian/Mahe |
| Africa/Freetown | Antarctica/Vostok | Indian/Maldives |
| Africa/Gaborone | Arctic/Longyearbyen | Indian/Mauritius |
| Africa/Harare | Asia/Aden | Indian/Mayotte |
| Africa/Johannesburg | Asia/Almaty | Indian/Reunion |
| Africa/Kampala | Asia/Amman | New_Salem |
| Africa/Khartoum | Asia/Anadyr | Pacific/Apia |
| Africa/Kigali | Asia/Aqtau | Pacific/Auckland |
| Africa/Kinshasa | Asia/Aqtobe | Pacific/Chatham |
| Africa/Lagos | Asia/Ashgabat | Pacific/Easter |
| Africa/Libreville | Asia/Baghdad | Pacific/Efate |
| Africa/Lome | Asia/Bahrain | Pacific/Enderbury |
| Africa/Luanda | Asia/Baku | Pacific/Fakaofo |
| Africa/Lubumbashi | Asia/Bangkok | Pacific/Fiji |
| Africa/Lusaka | Asia/Beirut | Pacific/Funafuti |

| | | |
|---|---|---|
| Africa/Malabo | Asia/Bishkek | Pacific/Galapagos |
| Africa/Maputo | Asia/Brunei | Pacific/Gambier |
| Africa/Maseru | Asia/Calcutta | Pacific/Guadalcanal |
| Africa/Mbabane | Asia/Choibalsan | Pacific/Guam |
| Africa/Mogadishu | Asia/Colombo | Pacific/Honolulu |
| Africa/Monrovia | Asia/Damascus | Pacific/Kiritimati |
| Africa/Nairobi | Asia/Dhaka | Pacific/Kosrae |
| Africa/Ndjamena | Asia/Dili | Pacific/Kwajalein |
| Africa/Niamey | Asia/Dubai | Pacific/Majuro |
| Africa/Nouakchott | Asia/Dushanbe | Pacific/Marquesas |
| Africa/Ouagadougou | Asia/Gaza | Pacific/Midway |
| Africa/Porto-Novo | Asia/Colombo | Pacific/Nauru |
| Africa/Sao_Tome | Asia/Ho_Chi_Minh | Pacific/Niue |
| Africa/Tripoli | Asia/Hong_Kong | Pacific/Norfolk |
| Africa/Tunis | Asia/Hovd | Pacific/Noumea |
| Africa/Windhoek | Asia/Irkutsk | Pacific/Pago_Pago |
| America/Adak | Asia/Jakarta | Pacific/Palau |
| America/Anchorage | Asia/Jayapura | Pacific/Pitcairn |
| America/Anguilla | Asia/Jerusalem | Pacific/Port_Moresby |
| America/Antigua | Asia/Kabul | Pacific/Rarotong |
| America/Araguaina | Asia/Kamchatka | Pacific/Saipan |
| America/Argentina/ | Asia/Karachi | Pacific/Tarawa |
| America/Argentina/ | Asia/Kathmandu | Pacific/Tongatapu |
| America/Argentina/Catamarca | Asia/Kolkata | Pacific/Wake |
| America/Argentina/Cordoba | Asia/Krasnoyarsk | Pacific/Wallis |
| America/Argentina/Jujuy | Asia/Kuala_Lumpur | UTC |
| America/Argentina/La_Rioja | Europe/Vaduz | New_Salem |
| America/Argentina/Mendoza | Asia/Kuwait | Mideast/Riyadh87 |
| America/Argentina/Rio_Gallegos | Asia/Macau | Mideast/Riyadh88 |

| | | |
|---|---|---|
| America/Argentina/Salta | Asia/Magadan | Mideast/Riyadh89 |
| America/Argentina/San_Juan | Asia/Makassar | America/Moncton |
| America/Argentina/San_Luis | Asia/Manila | America/Monterrey |
| America/Argentina/Tucuman | Asia/Muscat | America/Montevideo |
| America/Argentina/Ushuaia | Asia/Nicosia | Pacific/Tahiti |
| America/Aruba | Factory | America/Montserrat |
| America/Asuncion | Asia/Omsk | America/Nassau |
| America/Atikokan | Asia/Oral | America/New_York |
| Asia/Kuching | Asia/Phnom_Penh | America/Nipigon |
| America/Bahia | Asia/Pontianak | America/Nome |
| America/Barbados | Asia/Macau | America/Noronha |
| America/Belem | Asia/Magadan | America/North_Dakota/ |
| America/Belize | Asia/Makassar | America/North_Dakota/Center |
| America/Blanc-Sablon | Asia/Manila | America/Panama |
| America/Boa_Vista | Asia/Qatar | America/Pangnirtung |
| America/Bogota | Asia/Qyzylorda | America/Paramaribo |
| America/Boise | Asia/Riyadh | America/Phoenix |
| Asia/Novosibirsk | Indian/Antananarivo | America/Port_of_Spain |
| America/Cambridge_Bay | Asia/Riyadh89 | America/Port-au-Prince |
| America/Campo_Grande | Indian/Cocos | America/Porto_Velho |
| America/Cancun | Asia/Samarkand | America/Puerto_Rico |
| America/Caracas | Asia/Seoul | America/Rainy_River |
| Asia/Pyongyang | Asia/Shanghai | |
| America/Cayenne | Asia/Singapore | America/Moncton |
| America/Cayman | Asia/Taipei | Asia/Kabul |
| America/Chicago | Asia/Tashkent | Buenos_Aires |
| America/Chihuahua | Asia/Tbilisi | Canada/East-Saskatchewan |
| Asia/Riyadh87 | Asia/Tehran | ComodRivadavia |
| Asia/Riyadh88 | Asia/Samarkand | |

| | | |
|---|---|---|
| America/Costa_Rica | Asia/Thimphu | America/Regina |
| America/Cuiaba | Asia/Tokyo | America/Resolute |
| Asia/Sakhalin | Asia/Ulaanbaatar | America/Rio_Branco |
| America/Danmarkshavn | Asia/Urumqi | America/Santarem |
| America/Dawson | Asia/Vientiane | America/Santiago |
| America/Dawson_Creek | Asia/Vladivostok | America/Santo_Domingo |
| America/Denver | Asia/Yakutsk | America/Sao_Paulo |
| America/Detroit | Asia/Yekaterinburg | America/Scoresbysund |
| America/Dominica | Asia/Yerevan | America/St_Barthelemy |
| America/Edmonton | Atlantic/Azores | Asia/Kabul |
| America/Eirunepe | Atlantic/Bermuda | Buenos_Aires |
| America/El_Salvador | Atlantic/Canary | Canada/East-Saskatchewan |
| America/Maceio | Atlantic/Cape_Verde | ComodRivadavia |
| America/Managua | Asia/Urumqi | America/Recife |
| America/Fortaleza | Asia/Vientiane | America/Regina |
| America/Glace_Bay | Asia/Vladivostok | America/Resolute |
| Asia/Jerusalem | Atlantic/Faroe | America/Rio_Branco |
| America/Goose_Bay | Atlantic/Madeira | America/Santarem |
| America/Grand_Turk | Atlantic/Reykjavik | America/Santiago |
| America/Grenada | Atlantic/South_Georgia | America/Santo_Domingo |
| America/Guadeloupe | Atlantic/St_Helena | America/Sao_Paulo |
| America/Guatemala | Atlantic/Stanley | America/Scoresbysund |
| America/Guayaquil | Atlantic/Madeira | America/St_Barthelemy |
| America/Guyana | Atlantic/Reykjavik | America/Kentucky/Louisville |
| America/Halifax | Atlantic/South_Georgia | America/Kentucky/Monticello |
| America/Havana | Australia/Adelaide | America/La_Paz |
| America/Hermosillo | Australia/Brisbane | America/Lima |
| America/Indiana/Indianapolis | Australia/Broken_Hill | America/Los_Angeles |
| America/Indiana/Knox | Australia/Currie | America/Maceio |

| | | |
|---|---|---|
| America/Indiana/Marengo | Australia/Darwin | America/Managua |
| America/Indiana/Petersburg | Australia/Eucla | America/Manaus |
| America/Indiana/Tell_City | Australia/Hobart | America/Marigot |
| America/Indiana/Vevay | Australia/Currie | America/Martinique |
| America/Indiana/Vincennes | Australia/Lindeman | America/Mazatlan |
| America/Indiana/Winamac | Australia/Lord_Howe | America/Menominee |
| America/Manaus | Australia/Melbourne | America/Merida |
| America/Inuvik | Australia/Perth | America/Mexico_City |
| America/Iqaluit | Australia/Sydney | America/Miquelon |
| America/Jamaica | Asia/Jakarta | America/Kentucky/Louisville |
| America/Marigot | Asia/Jerusalem | America/Kentucky/Monticello |
| America/Juneau | Asia/Kabul | America/La_Paz |
| America/Lima | Asia/Kamchatka | Asia/Karachi |