Set Up the Cisco EPN Manager Server

These topics describe the tasks an administrator should perform after Cisco EPN Manager is installed. After these tasks are finished, users can log in and set up their working environment as described in Get Started With Cisco EPN Manager.

For information on the various types of Cisco EPN Manager users (for example, CLI and web GUI users), see How to Transition Between the CLI User Interfaces in Cisco Evolved Programmable Network Manager.

Note Be sure to review the important information in Best Practices: Harden Your Cisco EPN Manager Security.

- Server Setup Tasks, on page 1
- User Management Setup Tasks, on page 6
- Fault Management Setup Tasks, on page 7
- Web GUI Setup Tasks (Admin), on page 7

Server Setup Tasks

Task	See
Verify the backup settings	Set Up Automatic Application Backups
Install any required product licenses and software updates	Licenses and Software Updates
For software updates: • Enable notifications for product software updates (critical fixes, device support, add-ons) • Specify whether you want credentials stored on Cisco.com when Cisco EPN Manager checks for software updates, and if yes, whether you want the user to be prompted for credentials when checking for updates	Enable or Disable Notifications About Software Updates
Set up HTTPS on the server for secure interactions between the server and browser-based GUI client (you can use HTTP but HTTPS is recommended)	Secure the Connectivity of the Cisco EPN Manager Server

Task	See
Configure high availability	Configure and Manage High Availability
Adjust data retention and purging	Data Collection and Purging
For server-related traps that signal system problems, customize the threshold settings and severities, and forward the traps as SNMP trap notifications to configured receivers	Customize Server Internal SNMP Traps and Forward the Traps Forward Alarms and Events as SNMP Trap Notifications
Set up NTP (Network Time Protocol) so that time is synchronized between the server and network devices	Set Up NTP on the Server
Configure FTP/TFTP on the server for file transfers between the server and network devices	Enable FTP/TFTP/SFTP Service on the Server
Configure a proxy for the Cisco EPN Manager server	Set Up the Cisco EPN Manager Proxy Server
Configure the email server	Set Up the SMTP E-Mail Server
Enable the Compliance feature if you plan to use it to identify device configuration deviations	Enable and Disable Compliance Auditing
Enable the Service Discovery feature so that the Cisco EPN Manager discovers the services that are existing in the network and the services that are provisioned using the Provisioning Wizard.	Enable and Disable Service Discovery
Configure product feedback to help Cisco improve its products	Set Up Defaults for Cisco Support Requests

Configure and use LDAP/Active Directory Servers

Set Up User Authentication (TACACS+ and LDAP)

In addition to supporting local users, Cisco EPN Manager supports TACACS+ and LDAP users through integration with the TACACS+ and LDAP servers. The integration process has the following steps:

- Configure the TACACS+ and LDAP server.
- Create the roles that are referenced by the TACACS+ and LDAP users.
- Configure AAA settings.

Add an LDAP Server to Cisco EPN Manager

Lightweight Directory Access Protocol (LDAP) is a server protocol used to access and manage directory information. It manages directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer. It provides authentication with users who are listed in the LDAP directory and not specified in EPNM.

To add an LDAP server:

Step 1 From the main menu, select **Administration** > **Users** > **AAA** > **Servers** > **LDAP** tab. Using this window, you can add, edit settings, and delete a new LDAP server.

Note The following restrictions apply on values that you enter in the input fields listed in this page:

- No space at the beginning or at the end.
- The input string cannot start with '#'.
- The special characters: '+ * " ' / \ \\ < > ; ( ) \u0000 (Unicode Null character) \r' cannot be entered.

Step 2 Click the  icon.

Step 3 Enter the required LDAP Server Details—Server Address, Server Port, Password, IP address, DNS Name, and so forth.

Step 4 If you want to use the SSL communication channel, then check the **Use Secure Auth** check box. For more information about Installing LDAP certificates, see how to Configure LDAP Servers on the Cisco EPN Manager.

Note Set up HTTPS to secure the connectivity of the web server. This is a prerequisite before you configure LDAP with SSL. Administrator can configure the schema for each LDAP server.

Step 5 Enter the **Admin DN** string.

Step 6 Enter the **Password** and the **Confirm Password** details.

Note The LDAP administrator knows the string and confirmation password.

Step 7 Enter the schemas in the following fields: typically every LDAP server has its own configuration of users and groups and concatenated certificate file:

a) Subject Name Attribute—This value represents the *uid* attribute in the LDAP server user profile under which a particular username is organized.

b) Group Name Attribute—This value represents the role permissions that are assigned to the group members (admin, monitor, configurator), and is denoted by the *description* attribute in the LDAP server group profile.

c) Group Map Attribute—This value represents the association between group and user, and is denoted by the *memberUid* attribute in the LDAP server group profile.

Note To specify more than one user roles, in LDAP or Active Directory, you can create several attributes with same name or create one attribute and list multiple user roles separated by a comma. For example:

- To specify multiple attributes with same name:

```
description=Admin
description=Monitor Lite
```

- To specify one attribute and multiple user roles:

```
description=Admin,Monitor Lite
```

d) Virtual Domain Attribute—This value represents network sections that users can have access to, and is mentioned in the *title* attribute in the LDAP server user profile. This value is in relation with the Cisco EPN Manager virtual domain profiles configured in **Administration** > **Users** > **Virtual Domains** window. You can choose which elements should be included in a virtual domain and which users should have access to that virtual domain.

Note To specify more than one virtual domain, in LDAP or Active Directory, you can create several attributes with same name or create one attribute and list virtual domains separated by a comma. For example:

- To specify multiple attributes with same name:

```
description=VirtualDomain1
description=VirtualDomain2
```

- To specify one attribute and multiple user roles:

```
description=VirtualDomain1,VirtualDomain2
```

e) Subject Search Base—Specify the path to search where the users are located.
f) Group Search Base—Specify the path to search where the group are located.

Step 8 In the **Retries** field, enter the number of times that the LDAP authentication of source file can be run.

Step 9 Click **Save**.

Configure LDAP Servers on the Cisco EPN Manager

Cisco EPN Manager connects to the LDAP server using 1-way SSL. This means that you need to install the Certificate Authority (CA) root (and intermediate) certificates for the LDAP server in Cisco EPN Manager. You get these certificates from the CA for the LDAP server. The procedure below explains the steps to install the root (and intermediate) CA certificates.

Before you begin

Make sure to install the LDAP certificate to Cisco EPN Manager:

1. Get the root and intermediate certificates for the SSL certificate for the LDAP server, which is owned by the customer.
2. Log in as CLI admin user using ssh as mentioned in Establish an SSH Session With the Cisco EPN Manager Server.
3. Copy the CA root/intermediate certificate(s) for the LDAP server certificate to the local directory of Cisco EPN Manager. For example, copy your rootCA.pem to /localdisk/defaultRepo.
4. In the Cisco EPN Manager Admin CLI, run the command to import this CA root certificate in Cisco EPN Manager as - `EPNMServer/admin# ncs certvalidation trusted-ca-store importcacert alias <ALIAS> repository <Repository-name> <certificate-file> truststore {devicemgmt | pubnet | system | user}` (for example, `EPNMServer/admin# ncs certvalidation trusted-ca-store importcacert alias epnm40 repository defaultRepo certnew.cer truststore system`). This imports the LDAP certificate in the Java import trust store.
5. Restart Cisco EPN Manager.

Note If you have two LDAP servers and two Cisco EPN Manager servers (HA mode), install the root/intermediate certificate for each LDAP server and restart each Cisco EPN Manager server based on HA guidelines.

Step 1 Choose **Administration** > **Users** > **AAA** > **Settings**, **AAA Mode Settings** window appears.

Step 2 Choose the **LDAP** radio button.

Step 3 Check the **Enable Fallback to Local** check box to enable the use of the local database when the external AAA server is down.

Step 4 If you want to revert to local authentication if the external LDAP server goes down, perform the following steps:

a) Select **Enable Fallback to Local**.

b) Specify the fallback conditions—either **Only on no server response** or **On authentication failure or no server response**.

Note You should be able to log in as root users as they are authenticated locally.

Step 5 Click **Save All Changes**.

Note Use different browsers to log in to LDAP with the new user name and password.

Cisco WAN Automation Engine Integration with Cisco EPN Manager

The Cisco WAN Automation Engine (WAE) platform is an open, programmable framework that interconnects software modules, communicates with the network, and provides APIs to interface with external applications.

Cisco WAE provides the tools to create and maintain a model of the current network through continuous monitoring and analysis of the network and based on traffic demands that are placed on it. This network model contains all relevant information about a network at a given time, including topology, configuration, and traffic information. You can use this information as a basis for analyzing the impact on the network due to changes in traffic demands, paths, node and link failures, network optimizations, or other changes.

Note For details, refer to the latest *Cisco WAN Automation Engine (WAE) Installation Guide* and *Cisco WAN Automation Engine (WAE) User Guide*.

In Cisco EPN Manager, when you create an unidirectional or a Bidirectional tunnel with an explicit path, the WAN Automation Engine (WAE) integration provides you the explicit path using a REST call from Cisco EPN Manager automatically. Thus, you can avoid manually entering the explicit paths. WAE provides you a list of possible network paths to review and allows you to select an appropriate path.

Configure WAE Parameters

To specify the WAE path details:

Before you begin

Ensure to set the WAE parameters:

1. Choose **Administration** > **Settings** > **System Settings**
2. Expand Circuit VCs and then choose **WAE Server Settings**.

3. Enter the relevant WAE Details (version 7.1.3 and above) and field details such as **WAE Server IP**, **WAE Port Address**, **WAE Server User Name**, and **WAE Server Password**.

   If you want to use secure authentication, check the **Use Secure Auth** checkbox.

4. Click **Save** to save the WAE server settings or click **Reset to Defaults** to clear all the entries.

Step 1 Create a Unidirectional or Bidirectional tunnel with necessary parameters. For more information, see Create and Provision an MPLS TE Tunnel.

Step 2 In the **Path Constraints Details** area, choose the path type either as **Working** or **Protected**. See Field References for Path Constraint Details—MPLS TE Tunnel for descriptions of the fields and attributes.

Step 3 Check the **New Path** check box if you want to enable the **Choose Path from WAE server** check box.

Step 4 Check the **Choose Path from WAE server** checkbox. EPNM manager sends a REST request to WAE to obtain WAE networks.
WAE will return a list of possible networks.

Step 5 From the **Select WAE Network** drop-down list, choose a network.
EPNM manager will send a REST conf request to WAE with all the required parameters such as Source, Destination, and Network. Max path returned default value = 2; Max Path value is configured through WAE. WAE displays a list of possible paths satisfying the request.

Step 6 From the **Select WAE Path** drop-down list, choose the appropriate paths returned.
EPNM shows the selected path overlay on the map.

Step 7 Enter the name of the path in the **Path Name** field.
You can proceed with provisioning the order using the last selected path as explicit path.

User Management Setup Tasks

Task	See
Create web GUI users that have administration privileges, and disable the web GUI root account	Create Web GUI Users with Administrator Privileges Disable and Enable the Web GUI root User
Set up user authentication and authorization	Configure External Authentication Configure Local Authentication
Create user accounts and user groups	Control the Tasks Web Interface Users Can Perform
Adjust user security settings (password rules for local authentication, idle time logout setting)	Configure Global Password Policies for Local Authentication
Specify which users can approve jobs	Configure Job Approvers and Approve Jobs
Create virtual domains to control device access	Create Virtual Domains to Control User Access to Devices
Create a message that is displayed when users log in to the GUI client	Create a Login Banner (Login Disclaimer)

Fault Management Setup Tasks

Task	See
Forward alarms and events to other receivers in e-mail format	
Forward alarms and events to other receivers in SNMP trap format	Forward Alarms and Events as SNMP Trap Notifications
Configure global settings for alarm and event displays and searches: • Hide acknowledged, assigned, and cleared alarms in the Alarms and Events tables • Include acknowledged and assigned alarms in search results • Include device names in alarm messages	Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms
Customize the severity for specific events	Change Alarm Severity Levels
Customize the auto-clear interval for specific alarms	Change Alarm Auto-Clear Intervals
Make the text in the alarm **Failure Source** field more user-friendly	Change Alarm Severity Levels
Customize the behavior of expedited events	Change the Behavior of Expedited Events
Control generic event handling	Disable and Enable Generic Trap Processing
Control if and how users can create Cisco Support Requests	Set Up Defaults for Cisco Support Requests

Web GUI Setup Tasks (Admin)

Task	See
Disable features or menu items that your deployment does not use	Customize the Web GUI Menus to Disable Cisco EPN Manager Features, on page 7
Set Up the System Monitoring Administration Dashboard	Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard

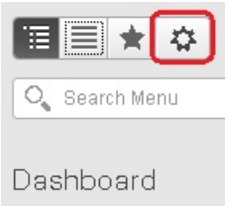
Customize the Web GUI Menus to Disable Cisco EPN Manager Features

If you belong to the root, Super Users, or Admin user group, you can customize Cisco EPN Manager so that specific menus are no longer displayed in the web GUI. See View User Groups and Their Members. This is

helpful if your deployment does not use all of the functions in Cisco EPN Manager. When you disable a menu, it is no longer displayed in the web GUI for any users, regardless of their user role.

Complete the following procedure to customize the web GUI by disabling entire features and specific menus. To re-enable the currently disabled features, use the same procedure, but toggle the feature's status to **Enabled** (or click **Enable All**).

Step 1 Click the gear that is displayed above the left sidebar menu.



Step 2 To disable an entire feature:

a. Locate the feature in the **Feature Navigation Groups** area.

b. In the feature's **Status** column, click the toggle so that it displays **Disabled**.

c. To check which menus will be disabled, scroll through the menus in the **Menu Details** area. All affected menus will be listed as **Disabled**.

Step 3 To disable specific menus:

a. Locate the menu in the **Menu Details** area.

b. In the menu's **Status** column, click the toggle so that it displays **Disabled**. If you disable a menu that has sub-menus, the sub-menus are also disabled. For example:

- If you disable **Group Management**, Cisco EPN Manager will disable all of the **Group Management** sub-menus: **Network Device Groups** and **Port Groups**.

c. To check which menus will be disabled, scroll through the menus in the **Menu Details** area.

Step 4 Click **Save**, then log out of the web GUI.

Step 5 Log back into the web GUI and validate your changes.