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 EPN 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 2
- Fault Management Setup Tasks, on page 3
- Web GUI Setup Tasks (Admin), on page 4

Server Setup Tasks

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**.
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	Disable and Enable the Web GUI root User
Set up user authentication and authorization	Configure External Authentication

Task	See
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)

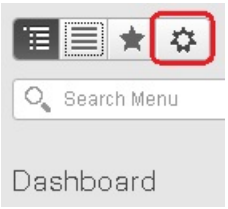
Task	See
Disable features or menu items that your deployment does not use	Customize the Web GUI Menus to Disable Cisco EPN Manager Features, on page 4
Set Up the System Monitoring Administration Dashboard	Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring 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**, **Compute Device Groups**, and **Port Groups**.

- If you disable only the **Compute Device Groups** sub-menu, Cisco EPN Manager will still display the **Network Device Groups** and **Port Groups** sub-menus under Group Management.

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.