Cisco Evolved Programmable Network Manager 7.0 User and Administrator Guide

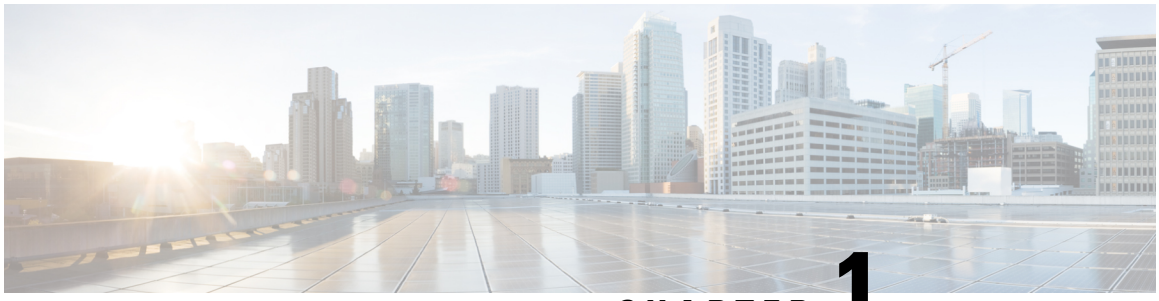
First Published: 2023-04-04

Last Modified: 2023-06-27

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

PART I

Get Started with Cisco EPN Manager



CHAPTER 1

Get Started With Cisco EPN Manager

Note If you are an administrator and need to set up Cisco EPN Manager for its initial use, see Server Setup Tasks, on page 687.

Web Client Requirements

The following are the client and browser requirements for the Cisco EPN Manager Web GUI:

- Hardware—Mac or Windows laptop or desktop compatible with one of the tested and supported browsers that are listed below.
- Browsers:

Note You can have up to three Cisco EPN Manager tabs open simultaneously in a single browser session.

- Google Chrome versions 70 onwards
- Mozilla Firefox ESR version 78

- Mozilla Firefox versions 70 onwards

- Recommended display resolution—1600x900 pixels or higher (minimum: 1366x768)

To improve loading time and reduce network bandwidth usage, Cisco EPN Manager caches static files (js, css) in the browser in the same version of Cisco EPN Manager (Firefox browsers).

Note Google Chrome ignores all caching directives and reloads page content because of known limitations about self-signed certificates.

Log In and Out

To log into the GUI, enter the following in your web browser address field, where *server-ip* is the IP address of the Cisco EPN Manager server:

https://*server-ip*

Note Do not autofill or save any username and password in the browser when you log in to Cisco EPN Manager.

Depending on your network configuration, the first time your browser connects to the Cisco EPN Manager web server, you may have to update your client browser to trust the security certificate of the server. You can also generate and import user-specific client certificates to your browser, which allows the user to log into Cisco EPN Manager. These generated client certificates allow you to log in without specifying a username or password. These generated client certificates require a passcode when you update them to your browser. This ensures the security of the connection between your client and the Cisco EPN Manager web server.

To log out, click ⚙ at the top right of the Cisco EPN Manager window and choose **Log Out**.

For information on Cisco EPN Manager users and the actions they can perform, see:

- How to Transition Between the CLI User Interfaces in Cisco Evolved Programmable Network Manager, on page 791 —Describes all classes of users supported by Cisco EPN Manager, including the various CLI user accounts.
- Types of User Groups, on page 793—Describes the user group mechanism which allows you to control the functions that everyday web GUI users can perform. What you can see and do in the user interface is controlled by your user account privileges. This topic also describes the virtual domain mechanism, which manages Role-Based Access Control (RBAC) for devices.

Setup Tasks to Complete Before Using Cisco EPN Manager

Before you can use the Cisco EPN Manager features, these tasks should be completed by an administrator:

Table 1: Setup Tasks and References

Tasks to complete before using Cisco EPN Manager	For information, see:
Setup and configure the Cisco EPN Manager server.	Server Setup Tasks, on page 687
Add devices to Cisco EPN Manager and create device groups to simplify device and network management.	Add and Organize Devices, on page 33
Enable monitoring for interfaces and technologies used by the network.	Monitor Device and Network Health and Performance, on page 223
Customize alarm and event behavior for your deployment (for example, alarm and event refresh rates, and e-mail and trap receivers).	Set Alarm and Event Management Preferences, on page 247

Change Your Password

To change your domain password,

- Click at the top right of the Cisco EPN Manager window and choose **Change Password** or navigate to **Administration** > **Users** > **Change Password**. Click the **?** (**Help**) icon to review the password policy.
- Enter the **Current Password** and the **New Password**. Confirm the new password.
- Click the **Change Password** button to save the password.

Use the Main Window Controls

The top left of the Cisco EPN Manager title bar provides the following controls.

	Menu button—Toggles the main Cisco EPN Manager navigation menu on the left (also called the left sidebar menu)
	Home button—Returns you to the home page (normally the Overview Dashboard)

The right side of the title bar displays your username and the virtual domain you are working in. A *virtual domain* is a logical grouping of devices. Virtual domains are used to control who has access to the devices and areas of the network. To switch between virtual domains that are assigned to you, see Work In a Different Virtual Domain , on page 23.

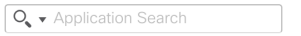
	Web GUI global settings—log out, change password, view your Cisco.com account profile, adjust your GUI preferences, check a Cisco.com support case, and so on.
	Current Server Time—displays the current server time and date.
	Online Help—launches the online help (User and Admin guide) for Cisco EPN Manager.
	Refresh—refreshes the page.

	Dock—opens a side dock window that displays your recent searches and navigational history.

The Alarm Summary gives you a visual indicator of number of alarms in your network. The color indicates the highest severity alarm.

	Alarm Summary—Provides a visual count of alarms in the categories that you specify. Clicking this area opens the **Alarm Summary** popup window.

When you click the **Alarm Summary** button, Cisco EPN Manager opens the **Alarm Summary** popup window. You can customize the data that is displayed in both the button and the pop-up window.

	Application Search—Global search tab that can be used to search the entire Cisco EPN Manager database. You can also use the filters for **Advanced Search** and **Saved Search**. **Note** Application Search cannot be used to search any data under **Raw Configuration Archive**.

Change Your Default Home Page

You can specify which page you want to display when you perform either of the following tasks:

- You click from the left side of the web GUI title bar.
- You log in to the Cisco EPN Manager web GUI.

This setting is saved on a per-user basis. You can change it at any time without affecting other users.

Step 1 While you have the page you want displayed, click at the top right of the Cisco EPN Manager web GUI.

Step 2 Choose **Set Current Page as Home**.

Set Up and Use the Dashboards

Dashboards provide at-a-glance views of the most important data in your network. They provide status, alerts, monitoring, performance, and reporting information. You can customize these dashboards so they contain only the information that is important to you. It may be helpful to set the **Network Summary** dashboard as your default home page. By doing so, this dashboard is displayed after you log in and you can quickly check overall network health before you do anything else. To set any dashboard as your default home page, see Change Your Default Home Page, on page 4.

Use the following dashboards to monitor and manage your network:

Note To view data on the dashboards, you must enable the relevant monitoring policies. By default, only device health monitoring (Device Health monitoring policy) is enabled. See How Device Health and Performance Is Monitored: Monitoring Policies, on page 223 for more information.

- **Network Summary** dashboard—To check the health of the entire network. See Network Summary Dashboard Overview.
- **Service Performance** dashboard—To monitor Carrier Ethernet and optical service performance. See Service Performance Dashboard Overview.
- **Performance** dashboard—To view high-level performance metrics for network components such as interfaces, QoS policies, and ITU-T Y.1731 probes. See Performance Dashboard Overview.
- **DWDM/OTN Performance** dashboard—To view performance information for the dense wavelength division multiplexing (DWDM) and Optical Transport Network (OTN) interfaces in your network. See DWDM/OTN Performance Dashboard Overview.

Users with administrator privileges can also use the following dashboards (**Administration** > **Dashboards**):

- **Licensing** dashboard—See View the Licensing Dashboard
- **Jobs** dashboard—See Manage Jobs Using the Jobs Dashboard, on page 23.
- **System Monitoring** dashboard—See Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard, on page 772.
- For details of the dashboard window and how to use dashboard filters, see How to Use the Dashboards, on page 18.
- To troubleshoot dashboard data issues, see Find Out Why Data Is Missing from a Dashboard.

Types of Dashboards

The following topics describe the dashboards available in Cisco EPN Manager.

Service Performance Dashboard Overview

From the **Service Performance** dashboard, you can view the performance statistics for a particular circuit, VC, or service during the time frame you specify. To open this dashboard, choose **Dashboard** > **Service Performance** > any of the tabs described in the following table.

Dashboard Tab	Information Provided
CEM	For the selected Circuit Emulation (CEM) circuit: • Details such as its name, type, and creation date • Statistics (you can toggle between the statistics for the circuit's endpoints) • Number of packets lost during transmission • Number of packets reordered in the jitter buffer before they reached their destination • Number of jitter buffer overruns and underruns • Number of packets ordered incorrectly and subsequently dropped • Number of malformed packets • Number of seconds that were errored, severely errored, or unavailable • Failed events • Dashlets that chart the number of Explicit Pointer Adjustment Relay counters (such L-bits and P-bits) that have been generated and received **Note** To view these dashlets, both the CEM and Pseudowire Emulation Edge to Edge monitoring policies must be enabled. See Monitoring Policies Reference, on page 949.
TE Tunnel	For the selected Traffic Engineering (TE) tunnel circuit: • Details such as its name, serviceability state, and associated endpoint • Service statistics • Outgoing traffic, bandwidth utilization, and reserved bandwidth • Service availability
SR Policy	For the selected Segment Routing (SR) policy: • Details such as its name, serviceability state, and associated endpoint • Service statistics • Outgoing traffic, bandwidth utilization, and reserved bandwidth • Service availability

Dashboard Tab	Information Provided

CE/L3VPN	For the selected circuit or VC:
	• Details such as its name, discovery state, and the last time it was modified
	• Lists the circuits and VCs with the highest values for the following parameters:
	  • Average traffic between endpoints
	  • QoS class traffic and drops
	Note You can toggle between inbound and outbound data. In the **Top N Service QoS Class Traffic** dashlet, you can also toggle between pre and postpolicy data.
	• Inbound and outbound QoS drops
	• Service traffic and availability
	• Two-way delay, one-way jitter, and service loss
	• End-to-end performance statistics for service probes with a cross-launch to the IPSLA dashboard for EVCs or to the Y.1731 dashboard for L3VPN services.

Top CE/L3VPN	Lists the circuits and VCs with the highest values for the following parameters: • Delay • Jitter • Service loss • Traffic (both inbound and outbound) You can toggle between CE and L3VPN services information. **Note** For large L3VPN circuits with more than 2000 endpoints, data cannot be displayed.

From release 7.0 onwards, for Cisco NCS 2000 series devices, Cisco EPN Manager utilizes the device timestamp data to store and display the historical PMON metric records. Earlier, local timestamp data was used, which displayed inaccurate (old) data in the graphs. Therefore, to avoid getting false data, always set the device timestamps to current date and time.

Note For a description of how to customize the contents and layout of a dashboard tab, see Customize a Dashboard Tab.

Performance Dashboard Overview

From the **Performance** dashboard, you can view high-level performance metrics for network components such as device, interfaces, QoS policies, and ITU-T Y.1731 probes. To open this dashboard, choose **Dashboard** > **Performance** > any of the tabs described in the following table.

Dashboard Tab	Information Provided
Device	For the selected device: • Device Memory Utilization Trend—displays the memory utilization graphs for the device. You can choose the required time frame and dates from the drop-down/checkboxes (Zoom and Date). • Device Memory Utilization Trend—displays the CPU utilization graphs for the device. You can choose the required time frame and dates from the drop-down/checkboxes (Zoom and Date). • Device Health information—displays various device health information such as temperature, alarms, events, and reachability. You can choose the required time frame and dates from the drop-down/checkboxes (Zoom and Date). • Device Port Summary—displays the port summary. You can click the **Down Ports** to view details about ports that are down. • Device Availability Trend—displays the device availability graphs (against time) for the device. You can choose the required time frame and dates from the drop-down/checkboxes (Zoom and Date). • Custom MIB Table View and Custom MIB Graph View—displays custom MIB information (if any).

Dashboard Tab	Information Provided

Interfaces	For the selected interface:
	• Details such as its name, the IP address of the device it is located on, and its configured speed.
	• The average, minimum, and maximum values for the following performance metrics (you can toggle between the metrics collected for inbound and outbound data):
	  • Traffic
	  • Utilization
	  • Errors
	  • Discards
	  • Cyclic redundancy check (CRC) errors
	  Note CRC error data is not polled by default. To enable the collection of this data, choose a polling frequency for the Interface Health monitoring policy's CRC parameter (see Change the Polling for a Monitoring Policy).
	• Individual graphs that chart the performance metrics listed in the **Interface Statistics** dashlet
	• Interface availability
	• Top N QoS class map policy graph (inbound and outbound prepolicy rate, postpolicy rate, and drops percentage)
	• QoS class map policy statistics (inbound and outbound)

QoS	For the selected QoS policy: • Summary information • Statistics and graphs for prepolicy, postpolicy, and dropped class map traffic. • Statistics and graphs for conforming, exceeding, and violating class map traffic
IP SLA	For Layer 3 services on the selected probe: • Summary information • IP Service Level Agreement (SLA) statistics • Delay, jitter, and frame loss between endpoints • Endpoint availability

Dashboard Tab	Information Provided
Y1731	For Layer 2 services on the selected probe: • Summary information • ITU-T Y.1731 statistics • Delay, jitter, frame loss, and CCM frame loss between endpoints • Jitter Bins Statistics • Delay Bins Statistics • Endpoint availability **Note** Bins statistics data is not polled by default. To enable the collection of this data, choose a polling frequency for Bins Statistics parameters in IP SLA Y.1731 Monitoring Policy (see Change the Polling for a Monitoring Policy).
BNG Statistics (deprecated)	Broadband Network Gateway (BNG) information for the selected device: • Details such as its name, IP address, product type, and software version • Names of configured IP pools, and the number and percentage of available addresses used by each pool • Chart that graphs the number of used or free addresses for the selected IP pools • Charts that graph the number of sessions for authenticated and up subscribers by line card and session type **Note** • Use the check boxes below the charts to select the items you want to view. • Place your cursor over any point in the graphs to view the values for the selected items at that particular time.

Dashboard Tab	Information Provided
ME1200 QoS (deprecated)	Quality of Service (QoS) information for the selected service on a Cisco ME 1200 device: • Details such as the name of the device, the customer associated with this device, and its user-network interface (UNI) port. • Average bit and frame rates for green (conforming), yellow (exceeding), red (violating), and discard traffic. You can toggle between inbound and outbound traffic data. • Graphs that chart the traffic measured for the traffic types listed in the **ME1200 QoS Statistics** dashlet. Note the following: • Five traffic graphs are provided: one for each traffic type and one consolidated graph. • You can toggle between viewing the data by frame rate (in frames per second) or bit rate (in kilobits per second). • You can specify the elements you want to view in a chart by checking the appropriate check box below that chart. In the consolidated traffic dashlet, you can specify traffic types. And in the individual traffic dashlets, you can specify one or multiple EVC Control Entries (ECEs) associated with the service.

Dashboard Tab	Information Provided

Optical SFPs	For the selected Small Form-Factor Pluggable (SFP) Transceiver Module interface:
	• Details such as its name, the name, and IP address of the device on which the interface is located, and its configured speed.
	• The average, minimum, and maximum values for the following operating metrics for a device:
	  • Optical input and output power
	  • Operating temperature
	  • Transceiver supply voltage
	  • Laser bias current
	For the selected Quad Small Form-Factor Pluggable (QSFP) Transceiver Module interface:
	Individual lane average, minimum, and maximum values for:
	  • Temperature
	  • Voltage
	  • Current
	  • Tx power
	  • Rx power
	• Individual graphs that chart the operating metrics listed in the **SFP Statistics** dashlet

Dashboard Tab	Information Provided

SONET/TDM Interfaces	For the selected SONET or time-division multiplexing (TDM) interface:
	• Details such as its name, configured speed, and the IP address of the device it is located on.
	• The average, minimum, and maximum values for the following performance metrics:
	  • Errored seconds
	  • Severely errored seconds
	  • C-bit severely errored seconds
	  • P-bit severely errored seconds
	  • Unavailable seconds
	  Values are provided for both the near-end (the receiving end) and far-end (the transmitting end) of the interface.
	• Individual graphs that chart the performance metrics listed in the **SONET/TDM Statistics** dashlet

Device Sensors	For each sensor of the selected device: • Name • Description • Measurement type • Current value Click the **i** icon on the current value to view the trend over last 6 hours.
MPLS Links Latency	You can get the following details for the link you select: • Link details such as the link name, endpoint device and interface. • Link delay (one-way and two-way). **Note** You can click Link Name in the Top N MPLS Links Table to launch the MPLS links dashboard on the selected link.

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- For a description of how to customize the contents and layout of a dashboard tab, see Customize a Dashboard Tab.

Network Summary Dashboard Overview

The **Network Summary** dashboard alerts you to the most important issues currently affecting your network. It also collects metrics from various sources to display a set of key performance indicators (KPIs). To open this dashboard, choose **Dashboard** > **Network Summary** > any of the tabs described in the following table.

Dashboard Tab	Information Provided
Network Devices	• Status (ICMP reachability, SNMP reachability, device manageability), system health, and alarm summary metric dashlets Note the following: • To open a pop-up window that describes the information provided by a metric dashlet, place your cursor over its name and then click the **?** icon. • To open a page that lists the alarms or devices that correspond to a particular metric, click a dashlet value. For example, if the **SNMP Reachability Status** dashlet indicates that 50 devices are currently reachable via SNMP, click **50** to open the **Network Devices** page and view a listing of these devices. • Top N devices by CPU utilization, memory utilization, and environmental temperature For the **Top N Environmental Temperature** dashlet, note the following: • Two temperature values are provided for each device: its highest recorded internal temperature (displayed in the **Max Inlet Temp** column) and its highest recorded ambient temperature (displayed in the **Max Other Temp** column). By default, devices are sorted by their internal temperature. • To identify the sensor that recorded a particular temperature value, place your cursor over its *i* (**information**) icon.

Dashboard Tab	Information Provided
Incidents	• System health and alarm summary metric dashlets Note the following: • To open a pop-up window that describes the information provided by a metric dashlet, place your cursor over its name and then click the **?** icon. • To open a page that lists the alarms that correspond to a particular metric, click a dashlet value. For example, if the **Alarm Summary** dashlet indicates that 12 critical alarms have been raised in your network, click **12** to open the **Alarms** page and view a listing of these alarms. • Alarm count for the entire network and the Cisco EPN Manager server • Top N alarm types • Syslog summary • Top N event types and their count • Top N devices by number of syslogs sent • Syslog details such as the corresponding device, severity, and message text • Top N devices by number of alarms raised
Top N Interfaces	For the selected port group: • Interface availability and utilization summaries • Top N devices by interface traffic, errors and discards, cyclic redundancy check (CRC) errors, and utilization **Note** CRC error data is not polled by default. To enable the collection of this data, choose a polling frequency for the Interface Health monitoring policy's CRC parameter (see Change the Polling for a Monitoring Policy). • Bottom N devices by interface availability Also note that the dashlets in this tab (except for the summary dashlets) allow you to open the 360 view for a device's adjacent device or interface by clicking its *i* (**information**) icon.
Top N QoS	For the selected port group: • Top N devices by QoS prepolicy, postpolicy, and drop rates • Top N devices by conforming, exceeding, and violating traffic rates You can toggle between inbound and outbound traffic data.

Dashboard Tab	Information Provided
Top N Y1731	Endpoints with the highest values for the following parameters: • Delay (one-way and two-way) • Jitter (one-way and two-way) • Frame loss
Top N MPLS Links Latency	• Delay (one-way and two-way) **Note** You can click Link Name in the Top N MPLS Links Table to launch the MPLS links dashboard on the selected link.
PTP/SyncE	• PTP Clock Class over time • Servo State over time • SyncE Quality Level over time **Note** Cisco EPN Manger uses the values that you have configured in the **PTP/SyncE** System Settings page to display data in the dashboard. See PTP/SyncE Dashboard Settings, on page 17 for more information.
GNSS	• GNSS Module Satellite ID and SNR details

You can view specific data by adding or removing columns in the dashlets. In the **Top N Interfaces**, **Top N QoS**, and **Top N Y1731** tabs, you can also use the **Sort by** option to sort the data displayed in the columns.

In the **Top N Interfaces** and **Top N QoS** tabs you can:

- Choose a specific device group and/or port group to view only information for those devices/ports.
  - To filter data for all the dashlets based on port/device groups, use the **Port Groups** filter at the top of the dashboard.
  - To filter data for a specific dashlet only, click the dashlet's **Edit** icon and choose a device/port group from the **Port Groups** and/or **Device Groups** drop-down list.
- Filter the data in the dashlets by Class Map (and you can choose to exclude the class-default).
- Filter the data in the dashlets using the **Time Frame** (default is Past 6 hours).
- Click an interface's name link to view performance information for that interface in the **Performance** dashboard. If you click a link in the **Top N Interfaces** tab, the **Interfaces** tab opens. If you click a link in the **Top N QoS** tab, the **QoS** tab opens instead.
- Interface monitoring is not enabled by default. For information on how to check this, see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- For a description of how to customize the contents and layout of a dashboard tab, see Customize a Dashboard Tab.

PTP/SyncE Dashboard Settings

To configure metrics that are used by Cisco EPN Manger to display data in the **PTP/SyncE** dashboard, navigate to **Administrator** > **System Settings** > **Performance** > **PTP/SyncE**. Configure the metrics as required and click **Save**.

Section	Description	Action
PTP Clock Class	Allows you to define the range of values of **PTP Clock Class** that should be reported as **Ok** or **Degraded** or **Failure**.	Enter values from the entire range of 0–255. Ensure that there is no overlap in values between the three categories.
PTP Servo State	Allows you to define how Cisco EPN Manager reports each of the five possible PTP Servo states.	Configure each of the five states in this section to **Ok** or **Degraded** or **Failure**.
SyncE Quality level	Allows you to define the SyncE quality levels that Cisco EPN Manager reports as Ok. By default, Cisco EPN Manger allows you to define two values as Ok. You can add a third value if required by selecting the check-box next to the grayed out field. Any other SyncE QL values apart from the ones that you have defined as **Ok** is reported as **Degraded**.	Choose a value from the drop-down list.
UTC Offset	You can define the correct UTC offset in the system. Cisco EPN Manger reports the devices configured with the matching value of UTC offset as **Correct UTC offset** and devices configured with offset not matching this value as **Incorrect UTC Offset**.	Enter a value between 0–65535.

DWDM/OTN Performance Dashboard Overview

The **DWDM/OTN Performance** dashboard displays performance information for the Dense Wavelength Division Multiplexing (DWDM) and Optical Transport Network (OTN) interfaces that are traversed by a specific circuit. This includes Circuit, Optical physical, Optical Data Unit (ODU), Optical Transport Unit (OTU), Ethernet, Synchronous Optical Network (SONET), and Synchronous Digital Hierarchy (SDH) interfaces.

To open this dashboard, perform one of the following actions:

- Choose **Dashboard** > **DWDM/OTN Performance** > **Circuit**. Click an interface name in the Interfaces dashlet. The relevant tab for the type of interface opens. For example, if you click an OTU interface, the OTU tab opens.
- From an Interface 360 view, choose **View** > **Performance**.

Note For IOS-XR devices, the dashboard displays performance information of the collected OTN 15 mins interface or the chosen specific OTN 15 mins parameter. The different parameters are:

- OTU FEnd
- OTU NEnd
- ODU FEnd
- ODU NEnd
- OTN GFP
- OTN FEC

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- For a description of how to customize the contents and layout of a dashboard tab, see Customize a Dashboard Tab.

How to Use the Dashboards

The following figure illustrates the key parts of a dashboard window and the controls that you can use to adjust them.

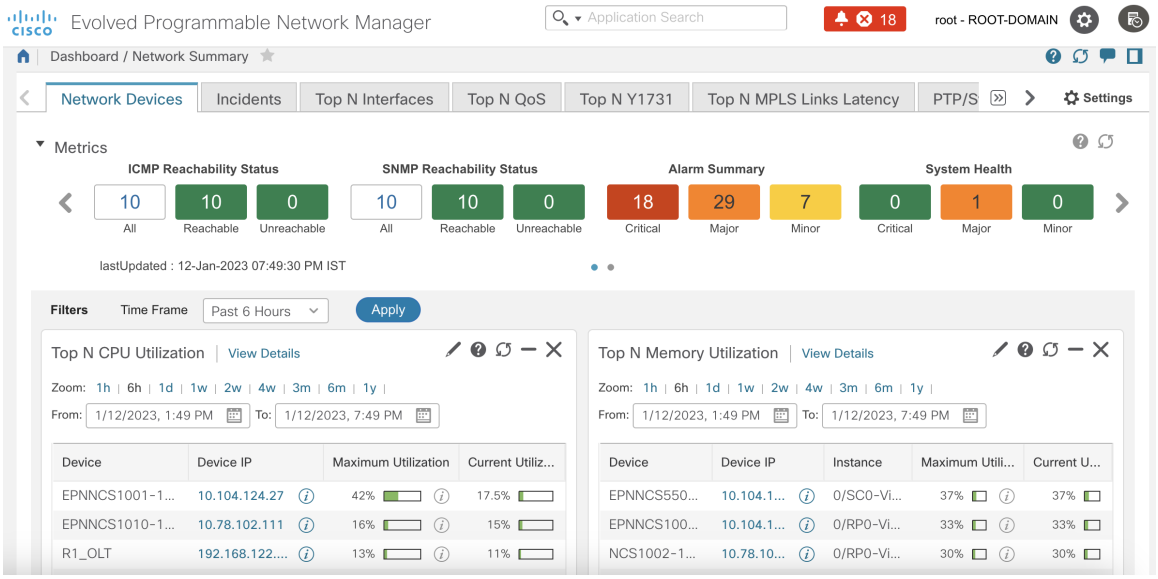
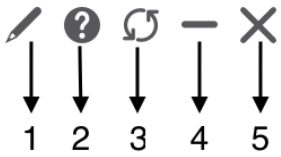


Table 2: Dashboard Elements

1	Dashboard filters—Filters all dashlets in the dashboard according to the selection. In this example, a time-based filter is used. The filters displayed depend on the dashboard type. For example, in the performance dashboards, you must select a specific interface, device, circuit, or VC.
2	Metric dashlets—Provides quick metrics for alarms, available devices, and so forth.
3	Dashboard settings and controls: • Dashboard icons—Allows you to launch online help, refresh the entire dashboard, provide feedback, and open the **Dock** window. • Dashboard **Settings** menu—Allows you to add or rename a dashboard tab, add new dashlets (both standard and metric), adjust the dashboard's layout, reset all dashboards to their default settings, and export data from the selected dashlets. **Note** The newly added or a renamed dashboard tab can be viewed only in the Tab view. This change is not reflected in the Dashboard menu.
4	Standard dashlets—Provides at-a-glance data that is relevant to the dashboard.

The top-right corner of each dashlet has icons that are activated when you use that dashlet. The dashlet type determines the icons that are available. The most common icons are displayed in the following figure:



1	**Edit** icon—Click to change a dashlet's properties, such as its title, refresh interval, and the number of devices that are displayed (applicable only to Top N and Bottom N dashlets).
2	**Help** icon—Click to open a pop-up window that describes the dashlet, indicates the monitoring policy that must be activated to collect data by the dashlet, and lists the filters that can be applied to the dashlet.
3	**Refresh** icon—Click to refresh the information displayed in the dashlet.
4	**Collapse/Expand** icon—Click to toggle between a maximized and minimized dashlet.
5	**Close** icon—Click to remove the dashlet from the dashboard.

The bottom-left corner of each dashlet has icons that can be used to change the display type of the data and export them. The most common icons are given in the following table:

Icon	Description
	• **Chart View**—Click to view the dashlet information as a chart. • **Table View**—Click to view the dashlet information as a table.

Icon	Description
	**Chart Type**—Click to choose the type of chart a dashlet displays (such as displaying a unique fill pattern for each element).
	**Actions**—Click to print the information provided by the dashlet or export the information.

You can also see the current date, time, and time zone, which is displayed in the standard time format of DD-MMM-YYYY hh:mm:ss AM/PM Z, where Z is the time zone.

Add a New Dashboard

Use this procedure to create a new dashboard. Your new dashboard appears as a new tab under one of the dashboards listed in Types of Dashboards, on page 5.

Step 1 Open the relevant existing dashboard.

For example, if you want to create a new tab under the **Performance** dashboard, click any tab under **Dashboard** > **Performance**.

Step 2 Click the **Settings** menu and choose **Add New Dashboard**.

Step 3 Enter a name for the new dashboard and click **Apply**.

Step 4 Click the new dashboard tab, and then add dashlets as described in Add a Predefined Dashlet To a Dashboard, on page 21.

Customize a Dashboard Tab

To customize a tab in any of the dashboards that Cisco EPN Manager provides, complete the following procedure:

Step 1 Choose the dashboard tab that you want to customize.

For example, if you want to customize the **Performance** dashboard's **Device** tab, choose **Dashboard** > **Performance** > **Device**.

Step 2 Adjust the dashboard tab as needed.

You can perform the following actions:

- Drag dashlets to a different location on the dashboard.
- From the tab's **Settings** menu, rename a tab, add new dashlets (see Add Dashlets to Dashboards), and change the tab's layout.

  The newly added or renamed dashboard tab can be viewed only in the Tab view. This change is not reflected in the Dashboard menu.

  Note To open a pop-up window that provides an overview of a dashlet you are thinking about adding, expand the **Add Dashlets** drop-down list, locate the dashlet, and then hover your cursor over its name.

- Use the filters to specify the information you want to view and the appropriate time frame, then click **Apply**.

Step 3 If necessary, troubleshoot why the tab is not displaying any data.

See Find Out Why Data Is Missing from a Dashboard for more information.

Add Dashlets to Dashboards

You can add two types of dashlets to your dashboards:

- Prepackaged dashlets that are provided with Cisco EPN Manager—Some of the dashlets are displayed on dashboards by default; others are listed in the **Settings** menu, and you can add them as needed. These dashlets provide information you will likely monitor (for example, device CPU utilization, interface errors and discards, and traffic statistics). See Add a Predefined Dashlet To a Dashboard, on page 21.

Add a Predefined Dashlet To a Dashboard

Cisco EPN Manager provides a predefined set of dashlets that provides you with commonly sought network data. By default, a subset of these dashlets is already included in the dashboards, to help you get started. Complete the following procedure to add another of these predefined dashlets to your dashboards.

Note To edit or remove a dashlet, click the appropriate icon from the top-right corner of that dashlet. (See How to Use the Dashboards.)

Step 1 From the sidebar menu, choose **Dashboard**, then select the dashboard you want to add a dashlet to.

For example, to add a **Device Memory Utilization** dashlet to the **Device** dashboard, choose **Dashboard** > **Performance** > **Device**.

Step 2 Identify the dashlet that you want to add, then add it:

a) From the top-right corner of the dashboard, click **Settings** and then click **Add Dashlet(s)**. Cisco EPN Manager lists the dashlets that can be added to that dashboard.

b) To open a pop-up window that provides an overview of a particular dashlet, hover your cursor over dashlet's name. The pop-up window also lists the sources for the data that the dashlet provides and the filters you can apply to the dashlet.

c) Click **Add** to add the selected dashlet to the dashboard.

Step 3 Verify that the dashlet is populated with data.

If it is not, check whether the required monitoring policy is enabled. (Only the Device Health monitoring policy is enabled by default. It checks device availability, CPU and memory pool utilization, and environmental temperature.)

a) From the top-right corner of the dashlet, click its **?** (**Help**) icon to open the dashlet's pop-up window.

b) Check the information provided in the **Data Sources** area. If it lists a monitoring policy, check whether the policy is activated. See Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.

Customize the Dock Window

Use the **Dock** window for quick navigation to frequently used web GUI pages and pop-up windows (such as the 360 view for a particular device). From here, you can also access links to the 15 most recently visited pages and Cisco EPN Manager training materials. To open this window, click the **Dock** icon (located in the top right area of the page).

Complete the following procedure to update the links provided in the **Dock** window:

Step 1 Add a web GUI page link to the **Favorites** tab (**Dock** icon > **Links Visited** > **Favorites**):

a) Open the web GUI page you want to add.
b) Click its star (**Favorite**) icon, which is located in the top left area of the page.

Step 2 Add a pop-up window link to the **Docked Items** area (**Dock** icon **> Docked Items**):

a) Open the pop-up window you want to add, then open its 360 view.
b) From the top right corner of the pop-up window, click the **Add to Dock** icon.

Find Out Why Data Is Missing from a Dashboard

If data is missing from a dashboard or dashlet, Cisco EPN Manager displays possible reasons in an error message in the dashlet such as:

- Monitoring policy not enabled
- Unmanaged or unreachable devices in the system
- Technology isn't supported on the device
- Inaccurate server time or server time not synced with the device

Perform the following steps to identify the cause:

Step 1 Check whether the dashlet data is filtered.

If you see **Edited** next to the dashlet name, do the following:

a) Click the **Edit** icon and adjust the current filter settings.
b) Click **Save and Close**.

Step 2 Check whether there is a problem with the device.

See Get Basic Device Information: Device 360 View, on page 84.

Step 3 Check whether the device inventory is being collected properly.

See Find Devices With Inventory Collection or Discovery Problems, on page 70.

Step 4 Check whether Cisco EPN Manager is collecting the required data by viewing the monitoring policies it is using:

a) Open the dashlet's overview pop-up window by clicking its **Help** icon.
b) Note the monitoring policy listed under **Data Sources**.
Monitoring policies are described in Monitoring Policies Reference, on page 949.
c) Verify that this policy is listed and active in the **Monitoring Policies** page.

To open this page, choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then choose **My Policies**.

- If the policy is not listed, proceed to Step 4d.
- If the policy is listed and its status is **Active**, click **Details** to open the **Collection Data** pop-up window and see if the device is being monitored by the policy. If it is not, you must adjust the policy as described in Change the Device Set a Policy is Monitoring, on page 234. If the device is included in the policy, proceed to Step 5.
- If the policy is listed and its status is **Inactive**, select the policy and click **Activate**.

d) Create a new monitoring policy and activate it.

See Adjust What Is Being Monitored, on page 230.

Step 5 Check whether the relevant data was purged from the system.

See How Data Retention Settings Affect Web GUI Data, on page 783.

Work In a Different Virtual Domain

Virtual domains are logical groupings of devices and are used to control your access to specific sites and devices. Virtual domains can be based on physical sites, device types, user communities, or any other designation the administer chooses. All devices belong to ROOT-DOMAIN, which is the parent domain for all new virtual domains. For more information about virtual domains, see Create Virtual Domains to Control User Access to Devices, on page 815.

If you are allowed access to more than one virtual domain, you can switch to a different domain by completing the following procedure:

Step 1 Click ⚙ from the right side of the title bar.

Step 2 Choose **Virtual Domain:** *current-domain*.

Step 3 From the **Virtual Domain** drop-down list, choose a different domain.

Cisco EPN Manager immediately changes your working domain.

Manage Jobs Using the Jobs Dashboard

If you have the appropriate user account privileges, you can manage Cisco EPN Manager jobs using the Jobs dashboard. To view the **Jobs** dashboard, choose **Administration** > **Dashboards** > **Job Dashboard**. From here, you can quickly see if a job was successful, partially successful, or failed.

If too many jobs are already running, Cisco EPN Manager will hold other jobs in the queue until resources are available. If this delays a scheduled job past its normal starting time, the job will not run. You will have to run it manually.

Some jobs may require approval. In such cases, Cisco EPN Manager sends an email to users with Administrator privileges notifying them that a job was scheduled and needs approval. The job will only run after it is approved. See Configure Job Approvers and Approve Jobs, on page 812.

You can set a time interval at which the jobs table is auto-refreshed. Click **Settings** in the upper corner of the page, select a value from the drop-down list in the field **Set Auto Refresh Rate** and click **Save**.

Note To disable auto-refresh of the jobs table, select OFF from the drop-down list.

The following table describes the buttons displayed in the **Jobs** dashboard.

Table 3: Jobs Dashboard Buttons

Button	Description
Delete Job	Removes a job from the **Jobs** dashboard.
Edit Job	Edit the settings configured for the selected job.
Edit Schedule	Displays the series schedule and lets you edit it (start time, interval, and end time). **Note** Editing the schedule of an already-scheduled job will change the status of that job to **Pending for Approval** since each edit requires an approval from the user who created the job.
Run	Runs a new instance of the selected job. Use this to rerun partially successful or failed jobs; the job will only run for the failed or partially successful components.
Abort	Stops a currently-running job, but allows you to rerun it later. Not all jobs can be aborted; Cisco EPN Manager will indicate when this is the case.
Cancel Series	Stops a currently-running job and does not allow anyone to rerun it. If the job is part of a series, future runs are not affected.
Pause Series	Pauses a scheduled job series. When a series is paused, you cannot run any instances of that series (using **Run**).
Resume Series	Resumes a scheduled job series that has been paused.

Note The **Delete Job**, **Abort**, and **Cancel Series** buttons are not available for system and poller jobs.

Note If you have logged in as a root user, then you can view all the jobs under Job Dashboard. If you have logged in as a non-root user, then you can only view the jobs performed by you.

To view the details of a job, follow these steps:

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 From the **Jobs** pane, choose a job series to get basic information (such as job type, status, job duration, and next start time).

Step 3 To view the job interval, click a job instance hyperlink.

At the top of the job page, the **Recurrence** field indicates how often the job recurs. Job interval details will be added for every job that triggers. The job details page is refreshed every 5 seconds until the job is completed.

Step 4 To get details about a failed or partially successful job, click the job instance hyperlink and expand the entries provided on the resulting page.

This is especially helpful for inventory-related jobs. For example, if a user imported devices using a CSV file (a bulk import), the job will be listed in the **Jobs** sidebar menu under **User Jobs** > **Device Bulk Import**. The job details will list the devices that were successfully added and the devices that were not.

Example

To troubleshoot a failed software image import job:

1. Choose **User Jobs** > **Software Image Import** from the **Jobs** sidebar menu.
2. Locate the failed job in the table and then click its hyperlink.
3. Expand the job's details (if not already expanded) to view the list of devices associated with the job and the status of the image import for each device.
4. To view the import details for a specific device, click that device's *i* (**information**) icon in the **Status** column. This opens an **Image Management Job Results** pop-up window.
5. Examine each step and its status. For example, the **Collecting image with Protocol: SFTP** column might report that SFTP is not supported on the device.

Change User Preferences

To change the User Preferences, click the icon at the top-right corner of the screen, and choose **My Preferences** > **General**.

Category	User Preference Setting	Description
List pages	**Items Per Page List**	Use this setting to define the number of entries displayed on the Monitoring pages for APs, Controllers, Site Maps, Roles & AAA > Active Sessions. By default, 50 entries are listed. **Note** This setting does not apply to Network Devices, Alarms and Events, configuration archive, software image management, or configuration.
Network Topology	**Automatically switch device group selection to show all participating devices**	Use this setting to automatically switch device group selection to view all participating devices in topology view. By default, this setting is not enabled.
	Auto-Refresh Interval (Map, Tables)	Use this setting to define the time interval at which the maps and tables in the network topology view are refreshed. You can set the refresh interval to 30 seconds, 1 minute, 2 minutes, or 5 minutes. Select **No auto-refresh** if you do not want to refresh the maps and tables. By default, the refresh interval is 1 minute.

Category	User Preference Setting	Description
Service Provisioning	**Default Technology**	Use this setting to define the Technology that is selected by default when you go to the service provisioning page to create a new service. **Note** If this user preference is not set, Carrier Ethernet will be set as the default value.
	Default Service Type	Use this setting to define the Service Type that is selected by default when you go to the service provisioning page to create a new service. **Note** If this user preference is not set, Access EPL will be set as the default value.
Chassis View Configuration	**UI Refresh Interval**	Use this setting to define how often the data in the UI is refreshed in the chassis view. By default, the UI refresh interval is 1 minute.
	Chassis racks to display	Use this setting to define the number of chassis racks Cisco EPN Manager should display. By default, this value is 2.
Device Inventory List View	**Device List Table Refresh Interval**	Use this setting to define the time interval at which the table in the Network Devices page is refreshed. You can set the refresh interval to 1 minute, 2 minutes, 5 minutes, 10 minutes, 15 minutes, or 30 minutes. Select **Do not refresh** if you do not want to refresh the table. The default value of this setting is **Do not refresh**.
Mobility Services Engine	**Use MSE Admin View**	By default, this setting is enabled.

Category	User Preference Setting	Description
User Idle Timeout	**Logout idle user**	Use this setting to define whether an idle user should be automatically logged out. By default, this option is enabled. **Note** To disable this setting, first ensure that the **Global idle user** is unchecked under **System Settings**.
	Logout idle user after	This setting also enables you to set the idle time for auto logout. By default, the value is 15 minutes. **Note** This value cannot exceed the value in the **Global Idle timeout** field under **System Settings**.

After you make the desired changes, click **Save** to apply your changed settings.

To clear the page level customization and setting, click **Clear GUI State Settings** on the top-right corner of the EPNM window. This deletes the custom settings made to Network Summary Dashboard, Performance Graphs, Network Devices, and so on, pages and refreshes the application to the default values.

For information about user preference settings in Alarms and Events, see Set Up Your Alarm and Event Display Preferences, on page 247.

Extend Cisco EPN Manager Functions

Advanced users can extend Cisco EPN Manager using the following tools:

- Cisco EPN Manager MTOSI API—Integrates Cisco EPN Manager with your Operations Support System (OSS).
- Cisco EPN Manager REST API—Manages additional administrative operations.

To get information about these tools, click ⚙ from the right side of the title bar and then choose **Help** > **API Help**. You can also download the following documents from Cisco.com:

- Cisco Evolved Programmable Network Manager MTOSI API Guide for OSS Integration
- Cisco Evolved Programmable Network Manager RESTCONF NBI Guide

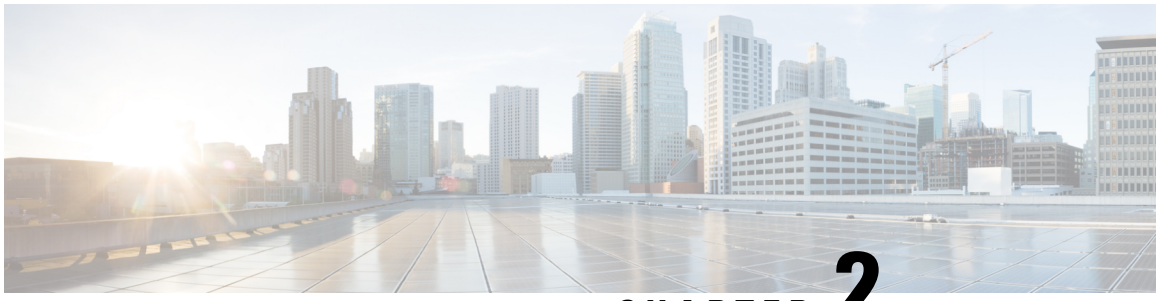
Check Cisco.com for the Latest Cisco EPN Manager Documentation

Refer to Cisco Evolved Programmable Network Manager Documentation Overview for information about and links to all of the documentation that is provided with Cisco EPN Manager.

Note We sometimes update the documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

PART II

Manage the Inventory



CHAPTER 2

Add and Organize Devices

Which Device Software Versions Are Supported by Cisco EPN Manager?

All devices should be running a *certified* device software version. However, certain devices must be running the *minimum* device software version. Follow the instructions in the table below on how to find out about a device software version.

To find this information:	**Do the following:**
A list of all certified device software versions	Refer to Cisco EPN Manager.
	Choose **Help** > **Supported Devices** and hover over the "i" in the **Software Version** column to display a popup.

Devices that require a minimum device software version	Choose **Help** > **Supported Devices** and check the **Software Version** column for text similar to **>=x.x** (For example, **>=12.2** would indicate that the device must run at least device software version 12.2).

Generic Device Support

The Cisco EPN Manager provides management of generic Cisco and non-Cisco devices, which are not officially supported (features).

Table 4: Generic Device Support

Generic Device Type	Supported Features	Supported MIBs	Supported Faults
Cisco device	System - Summary System - Environment System - Civic Location System - Modules System - Physical Ports System - Sensor Interfaces - All Interfaces Interfaces - Ethernet Interfaces Physical Links	SNMPv2 ENTITY-MIB IF-MIB LLDP-MIB CISCO-ENTITY-FRU-CONTROL-MIB	Linkup/ Linkdown (IF-MIB) Warm start (SNMPv2-MIB) Cold start (SNMPv2-MIB) Authentication Failure (SNMPv2-MIB) BDI interface down/ up (Link down/up localized to BDI) (IF-MIB) entSensorThresholdNotification (CISCO-ENTITY-SENSOR-MIB)
Non-Cisco device	System - Summary System - Modules System - Physical Ports Interfaces - All Interfaces Physical Links	SNMPv2 ENTITY-MIB IF-MIB LLDP-MIB	Linkup/ Linkdown (IF-MIB) Warm start (SNMPv2-MIB) Cold start (SNMPv2-MIB) Authentication Failure (SNMPv2-MIB)

Generic Device Support: Map a New Generic Device

You can manage a generic device by mapping it to a Cisco device to support functionalities such as inventory management, device level configuration, service provisioning, topology discovery, and fault management.

Note The Cisco device that you intend to map with a generic device must have a similar parity and version level.

To map a new generic device to a Cisco device,

Step 1 Navigate to **Administration** > **Settings** > **System Settings** > **Inventory**, and choose **Inventory**.

Step 2 Click the "+" icon under **Custom Device Profile** to open an **Add Custom Device Profile** window.

Step 3 Enter the Product OID, Original Device Type, and Existing Device Profile Tree (Cisco device type).

Step 4 Once the mapping is complete, go to **Network devices**, add the newly mapped generic device and manage it. See Add and Organize Devices, on page 33.

Note Chassis View is not available for any mapped generic device.

Generic Device Support: Map an Existing Generic Device

You can map an existing generic device to a Cisco device to extend the support for functionalities such as inventory management, device level configuration, service provisioning, topology discovery, and fault management.

Note The Cisco device type that you intend to map with a generic device must have the similar parity and version level.

To map an existing generic device to a Cisco device,

Step 1 Navigate to **Administration** > **Settings** > **System Settings** > **Inventory**, and choose **Inventory**.

Step 2 Click the "+" icon under **Custom Device Profile** to open an **Add Custom Device Profile** window.

Step 3 Enter the Product OID, Original Device Type, and Existing Device Profile Tree (Cisco device type).

Step 4 Once the mapping is complete, go to **Network devices** and click the **Sync** option. This completes the mapping procedure and syncs the generic device with its mapped Cisco device type.

Note Chassis View is not available for any mapped generic device.

Inventory Discovery Process

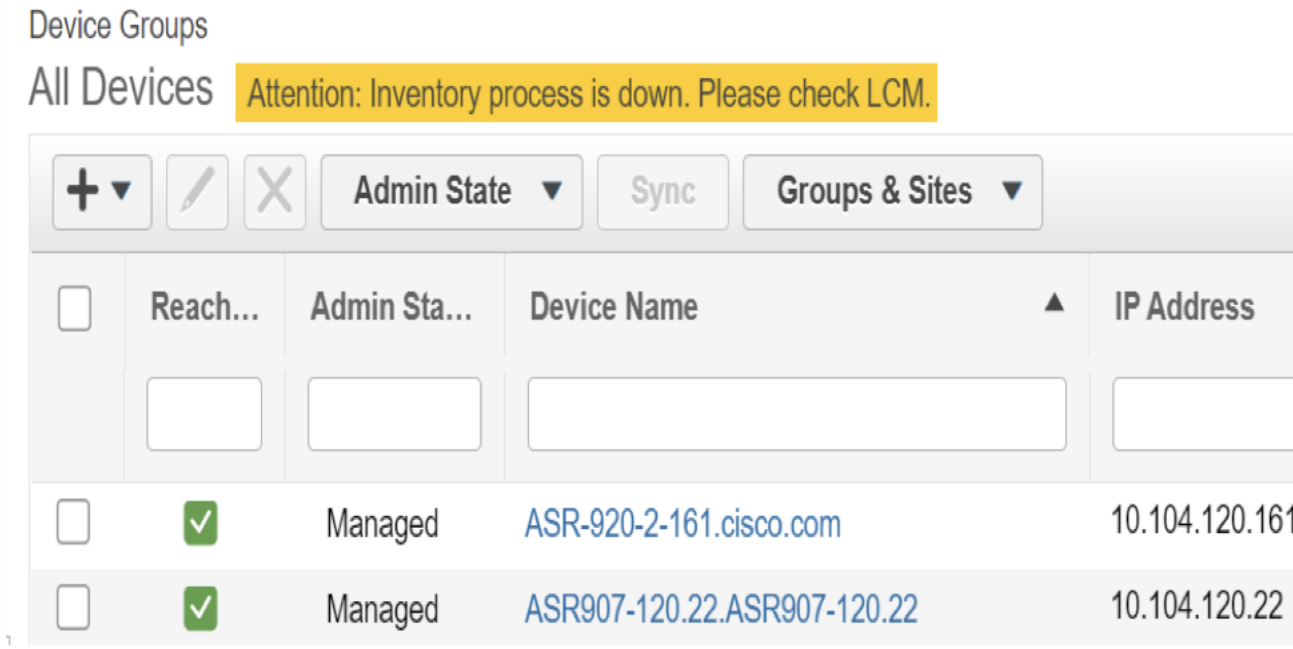
To enable scaling of devices in Cisco EPN Manager, the inventory discovery component of the EPNM process is run as a separate process (inventory-discovery-process). All functions related to inventory collection (including adding or importing devices, manual sync, granular and reactive sync, failed feature sync, switch inventory, and user-defined inventory discovery) are performed by inventory-discovery-process.

Note Configurations done through an open config interface in IOS-XR devices are not discovered in EPNM.

What happens when inventory-discovery-process is down

Cisco EPN Manager displays an error message in the **Network Devices** page when inventory-discovery-process is down.

Note You will not be able to perform any inventory operations when the inventory-discovery-process is down. Please wait for the process to come up before resuming any inventory operations.



Logs related to inventory-discovery-process are stored at `/opt/CSCOlumos/logs/inventory-discovery-process`. See Inventory Discovery Process Logs, on page 869 for more information.

The status of inventory-discovery-process (started, stopped, reachable, unreachable, and restarting) is displayed as a system-generated event in the **Monitor** > **Alarms and Events** page.

For example, the event "Process inventory-discovery-process is unreachable and will try to restart" indicates that inventory-discovery-process is not reachable and will be restarted automatically.

Important The event "Process inventory-discovery-process reached auto-restart limit" indicates that the inventory-discovery-process has failed to restart automatically inspite of multiple retries. In this case, it is recommended that you open a support case with Cisco Technical Assistance Center (TAC). See Open a Cisco Support Case, on page 861.

Add Devices to Cisco EPN Manager

Cisco Evolved Programmable Network Manager uses device, location, and port groups to organize elements in the network. When you view devices in a table or on a map (network topology), the devices are organized in terms of the groups they belong to. When a device is added to Cisco EPN Manager, it is assigned to a group named **Unassigned Group**. You can then move the device into the desired groups as described in Create Groups of Devices for Easier Management and Configuration, on page 72.

Note

- To add a Cisco WLC to Cisco EPN Manager, make sure it does not have any unsupported Access Points (APs), otherwise Cisco EPN Manager will not discover any APs from that WLC.
- Cisco EPN Manager does not support multiple independent networks that share the same IP addresses. Ensure the network element that you add does not contain conflicting IP addresses.

Table 5: Methods for Adding Devices

Supported Methods for Adding Devices	See:
Add multiple devices by discovering the neighbors of a seed device using:	Add Devices Using Discovery, on page 38.
• Ping sweep and SNMP polling (Quick Discovery)	• Run Quick Discovery, on page 39
• Customized protocol, credential, and filter settings (useful when you will be repeating the discovery job)	• Run Discovery with Customized Discovery Settings, on page 40
Add multiple devices using the settings specified in a CSV file	Import Devices Using a CSV File, on page 42.
Add a single device (for example, for a new device type)	Add Devices Manually (New Device Type or Series), on page 44

These topics provide examples of how to add a Carrier Ethernet and an Optical device to Cisco EPN Manager:

- Example: Add a Single Cisco NCS 2000 or NCS 4000 Series Device, on page 45
- Example: Add a Network Element as an ENE Using Proxy Settings, on page 45

Add Cisco ME1200 devices in Cisco EPN Manager

Follow these settings while adding Cisco ME1200 devices in Cisco EPN Manager:

- SNMP - Use the same SNMP settings as that of other devices.
- CLI - Ensure that the protocol setting is set to SSH2. Though the device can be reached via telnet using a port, it is recommended to use SSH protocol. If telnet is used, then the custom telnet port used must be 2323.

- Remember that configuration changes to Cisco ME1200 devices are not automatically discovered by Cisco EPN Manager. After making a change, you must manually sync the device. To do this, select the required device (s) in the Network Devices table and click **Sync**.

Add Devices Using Discovery

Cisco EPN Manager supports two discovery methods:

- Ping sweep from a seed device (Quick Discovery). The device name, SNMP community, seed IP address and subnet mask are required. This method is not supported for discovering optical devices. See Run Quick Discovery, on page 39
- Using customized discovery methods (Discovery Settings)—This method is recommended if you want to specify settings and rerun discovery in the future. If you want to discover optical devices, use this method. See Run Discovery with Customized Discovery Settings, on page 40.

Note

- If a discovery job rediscovers an *existing* device and the device's last inventory collection status is **Completed**, Cisco EPN Manager does *not* overwrite the existing credentials with those specified in the Discovery Settings. For all other statuses (on existing devices), Cisco EPN Manager overwrites the device credentials with those specified in the Discovery Settings.
- Service discovery might take longer than usual when a large number of devices is added during database maintenance windows. Therefore, we recommend that you avoid large-scale operations during the night and on weekends.
- Autonomous APs are filtered out of the discovery process to optimize the discovery time. You need to manually add Autonomous APs using Import Devices or Credential Profile.

The discovery process of a device is carried out in the sequence of steps listed below. As Cisco EPN Manager performs discovery, it sets the reachability state of a device, which is: Reachable, Ping Reachable, or Unreachable. A description of the states is provided in Device Reachability and Admin States, on page 66.

1. Cisco EPN Manager determines if a device is reachable using ICMP ping. If a device is not reachable, its reachability state is set to **Unreachable**.
2. Server checks if SNMP communication is possible or not.
   - If a device is reachable by ICMP but its SNMP communication is not possible, its reachability state is set to **Ping Reachable**.
   - If a device is reachable by both ICMP and SNMP, its reachability state is **Reachable**.
3. Verifies the device's Telnet and SSH credentials. If the credentials fail, details about the failure are provided in the Network Devices table in the **Last Inventory Collection Status** column (for example, **Wrong CLI Credentials**). The reachability state is not changed.
4. Modifies the device configuration to add a trap receiver so that Cisco EPN Manager can receive the necessary notifications (using SNMP).
5. Starts the inventory collection process to gather all device information.
6. Displays all information in the web GUI, including whether discovery was fully or partially successful.

Note When Cisco EPN Manager verifies a device's SNMP read-write credentials, the device log is updated to indicate that a configuration change has been made by Cisco EPN Manager (identified by its IP address).

Verify SNMP Communication

Follow these steps if the reachability state of a device is set as **Ping Reachable**.

Note For Cisco NCS 2000 devices, verify the TL1 credentials, in addition (or instead) to SNMP credentials.

Step 1 Ensure that the credentials used by Cisco EPN Manager for device verification are correct.

Step 2 Verify that SNMP is enabled on the device and that the SNMP credentials configured on the device match those configured on Cisco EPN Manager.

Step 3 Check whether SNMP packets are being dropped due to configuration errors or due to your security settings (default behavior) in all the network devices that are participating in transporting SNMP packets between the managed devices and the Cisco EPN Manager server.

Specify the Management IP Address Type (IPv4/IPv6) for Discovered Devices

For discovered dual-home (IPv4/IPv6) devices, specify whether you want the Cisco EPN Manager to use IPv4 or IPv6 addresses for management IP addresses.

Note Device inventory has a limited DNS name IPv6 support.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Network Discovery**.

Step 2 From the **IPv4/IPv6 Preference for Management Address** options, choose either **IPv4** or **IPv6**.

Note Ensure that the management IP address that you choose is not a combination of IPv4 and IPv6 addresses.

Step 3 Click **Save**.

Run Quick Discovery

Use this method when you want to perform a ping sweep using a single seed device. Only the device name, SNMP community, seed IP address and subnet mask are required. If you plan to use the configuration management features, you must provide the protocol, user name, password, and enable password.

Before you begin

See Configure Devices So They Can Be Modeled and Monitored, on page 53 to make sure your devices are configured correctly.

Step 1 Choose **Inventory** > **Device Management** > **Discovery**, then click the **Quick Discovery** link at the top right of the window.

Step 2 At a minimum, enter the name, SNMP community, seed IP address, and subnet mask.

Step 3 Click **Run Now**.

What to do next

Click the job hyperlink in the **Discovery Job Instances** area to view the results.

Run Discovery with Customized Discovery Settings

Cisco EPN Manager can discover network devices using discovery profiles. A discovery profile contains a collection of settings that instructs Cisco EPN Manager how to find network elements, connect to them, and collect their inventory. For example, you can instruct Cisco EPN Manager to use CDP, LLDP, OSPF to discover devices, or just perform a simple ping sweep (an example of the results of a ping sweep is provided in Sample IPv4 IP Addresses for Ping Sweep, on page 41.) You can also create filters to fine-tune the collection, specify credential sets, and configure other discovery settings. You can create as many profiles as you need.

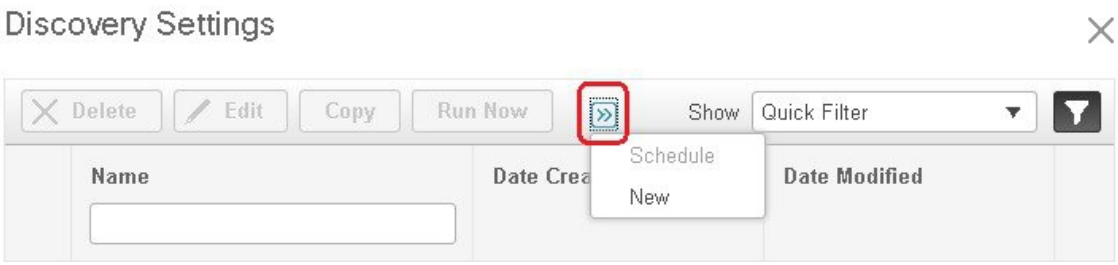
After you create a profile, create and run a discovery job that uses the profile. You can check the results of the discovery job on the **Discovery** page. You can also schedule the job to run again at regular intervals.

Before you begin

See Configure Devices So They Can Be Modeled and Monitored, on page 53 to make sure your devices are configured correctly so that Cisco EPN Manager can discover them.

Step 1 Choose **Inventory > Device Management > Discovery**, then click the **Discovery Settings** link at the top right of the window. (If you do not see a Discovery Settings link, click the arrow icon next to the Quick Discovery link.)

Step 2 In the **Discovery Settings** pop-up, click **New**.



Step 3 Enter the settings in the **Discovery Settings** window. Click "**?**" next to a setting to get information about that setting. For example, if you click "**?**" next to **SNMPv2 Credential**, the help pop-up provides a description of the protocol and any required attributes.

Step 4 Click **Run Now** to run the job immediately, or **Save** to save your settings and schedule the discovery to run later.

Sample IPv4 IP Addresses for Ping Sweep

The following table provides an example of the results of a ping sweep.

Subnet Range	Number of Bits	Number of IP Addresses	Sample Seed IP Address	Start IP Address	End IP Address
255.255.240.0	20	4094	205.169.62.11	205.169.48.1	205.169.63.254
255.255.248.0	21	2046	205.169.62.11	205.169.56.1	205.169.63.254
255.255.252.0	22	1022	205.169.62.11	205.169.60.1	205.169.63.254
255.255.254.0	23	510	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.0	24	254	205.169.62.11	205.169.62.1	205.169.63.254
255.255.255.128	25	126	205.169.62.11	205.169.62.1	205.169.63.127
255.255.255.192	26	62	205.169.62.11	205.169.62.1	205.169.63.62
255.255.255.224	27	30	205.169.62.11	205.169.62.1	205.169.63.30
255.255.255.240	28	14	205.169.62.11	205.169.62.1	205.169.63.14
255.255.255.248	29	6	205.169.62.11	205.169.62.9	205.169.63.14
255.255.255.252	30	2	205.169.62.11	205.169.62.9	205.169.63.10
255.255.255.254	31	0	205.169.62.11		
255.255.255.255	32	1	205.169.62.11	205.169.62.11	205.169.62.11

Example: Add Optical Devices Using Discovery

The following example shows how to use a seed device and the OTS protocol to discover Cisco NCS 2000 devices.

Before you begin

Check Configure Devices So They Can Be Modeled and Monitored, on page 53 to make sure the optical devices are configured correctly.

Step 1 Choose **Inventory** > **Device Management** > **Discovery**, then click the **Discovery Settings** link at the top right of the window.

Step 2 In the **Discovery Settings** window, click **New** to create a new discovery profile.

a) Enter a discovery profile name.

b) Enter the seed device and hop count information for the OTS protocol.

1. Click **Advanced Protocols** to open the discovery protocols list.

2. Click the **OTS Topology** drop-down to open the OTS protocol window.
3. Check the **Enable OTS** check box.
4. Click the Add Row ("+") icon.
5. Enter the seed device IP address and hop count (for example, **209.165.200.224** and **3**), then click **Save** to add the seed device information.
6. Click **Save** and close the window.

c) Enter the TL1 device credentials for the Cisco NCS 2000 series seed device.

1. In the **Credential Settings** area, click the **TL1 Credential** drop-down list to open the TL1 credentials window.
2. Click the Add Row ("+") icon.
3. Enter the seed device IP address, username, password, and proxy IP address (if required).
4. For Secure TL1 access, choose **Enable** from the **SSH** drop-down list. For Unsecured TL1, choose **Disabled**.
5. Click **Save** to add the credential information.
6. Click **Save** and close the window.

Step 3 Click **Save** to save the new discovery profile. The new **NCS2k_3_OTS** profile is added to the Discovery Settings window.

Note If you receive an error message, make sure you have enabled the protocols. (This is a common error.)

Step 4 Select **NCS2k_3_OTS**, then click **Run Now** to begin the discovery job.

Step 5 Check the results of the job by choosing **Inventory** > **Device Management** > **Discovery**.

Import Devices Using a CSV File

Use a CSV file to add devices if you have an existing management system from which you want to import devices, or you want to specify different values in a spreadsheet.

- Create the CSV File, on page 42
- Import the CSV File, on page 43

Create the CSV File

Follow this procedure to create the CSV file.

Step 1 Create the bulk import CSV file using the template that is available from the **Bulk Import** dialog box. To open the dialog box, choose **Inventory** > **Device Management** > **Network Devices**, click the + icon above the Network Devices table, and choose **Bulk Import**. Use the bulk device add sample template.

Step 2 To find out what the different fields mean and which fields are required, use the information that is in the web GUI. The information is the same for adding a single device or adding devices in bulk. To get this information, choose **Inventory** > **Device Management** > **Network Devices**, click the + icon above the Network Devices table, then choose **Add Device**. Mandatory fields are indicated by an asterisk; fields that require an explanation display a **?** icon next to them (hover your cursor over the **?** icon to view the field details).

Step 3 When you are done, save your changes and note the location of the file so you can import it as described in Import the CSV File, on page 43.

Import the CSV File

Follow this procedure to import and add devices using a CSV file.

Before you begin

See Configure Devices So They Can Be Modeled and Monitored, on page 53 to make sure your devices are configured correctly.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 Click the + icon above the Network Devices table, then choose **Bulk Import**.

Step 3 In the **Bulk Import** dialog:

a) Make sure **Device** is chosen from the **Operation** drop-down list.

b) Click **Browse**, navigate to the CSV file, then click **Import**.

Note Choose the CSV file that you have exported already as part of bulk device add sample template download. Do not edit the csv file manually.

Step 4 Check the status of the import by choosing **Administration** > **Dashboards** > **Job Dashboard**.

Step 5 Click the arrow to expand the job details and view the details and history for the import job. If you encounter any problems, see Validate Added Devices and Troubleshoot Problems, on page 69.

How Groups Work during Import

Note the following points about device groups during import:

- Before adding devices, check whether all device groups mentioned in the CSV file are present in Cisco EPN Manager.
- If a group associated with a device is not present, Cisco EPN Manager adds that device without mapping it to the group.
- Cisco EPN Manager retains any existing group mapping from before the import.
- If the CSV file contains both existing and new group mapping for a device, Cisco EPN Manager associates the device to the new groups in addition to the existing groups.
- Cisco EPN Manager lists devices added through the **Bulk Import** option under the **Add Device Manually** area, even if the associated device group has dynamic rules.
- To complete the device group mapping, perform synchronization after the import is complete. From the **Network Devices** table, select the devices, and click **Sync**.

Add Devices Manually (New Device Type or Series)

Use this procedure to add a new device type and to test your settings before applying them to a group of devices.

Before you begin

See Configure Devices So They Can Be Modeled and Monitored, on page 53 to make sure your devices are configured correctly.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 Click the + icon above the Network Devices table, then choose **Add Device**.

Step 3 In the **Add Device** dialog box, complete the required fields. Click the **?** icon next to a field for a description of that field. Ensure that you assign your devices to the relevant network role by selecting an option under Device Role.

Note Telnet/SSH information is mandatory for devices such as most Cisco NCS devices. Even if the default timeout for Telnet/SSH (60 sec) and SNMP (10Sec) differ between devices based on the network latency, the devices can be configured.

You can mandate the SSH key validation for the added device, by selecting the **Strict host check key for SSH** check box in the **Administration > Settings > System Settings > Inventory> Inventory** page. This enables you to specify the algorithm and SSH key under Telnet/SSH Parameters.

If you do not want to manually specify the algorithm and SSH key while adding the device, select the **Trust SSH key on first use** check box in the **Administration >Settings > System Settings > Inventory> Inventory** page. The SSH key sent from the device during its first communication will be trusted and added to the device credentials. This saved key will be auto populated when the device is added in future and used for validation.

Step 4 (Optional) Click **Verify Credentials** to validate the credentials before adding the device.

Step 5 Click **Add** to add the device with the settings you specified.

Note For NCS 2000 devices, provide a TL1 user with SuperUser profile, otherwise the devices will go to **Completed with Warning** status and the **Configuration > Security** tab will not be available in **Chassis View**.

Note Not providing Telnet/SSH credentials may result in partial collection of inventory data.

Note For NCS 2000 devices, the **Enable Single Session TL1** setting takes effect only for devices running release 11.0 onwards.

Note Cisco EPN Manager, by default, does not accept UCS with self-signed certification. User can enable it manually by adding the following lines in the */opt/CSCOlumos/xmp_inventory/xde-home/inventoryDefaults/ncsCIMC.def* file.

```
<default attribute="HTTPS_TRUST_CONDITION">always</default>

<default attribute="HTTPS_HOSTNAME_VERIFICATION_STRATEGY">allow_all</default>
```

Note Each device must have a Unique SNMP Engine ID. If same Engine Id is used in two devices, an alarm will be raised with conflicting device details. The SNMP Engine Id's unique check will happen only if we manage the device with SNMP v3 credentials.

Example: Add a Single Cisco NCS 2000 or NCS 4000 Series Device

Cisco NCS 2000 series devices are TL1-based devices, and Cisco Evolved Programmable Network Manager uses the TL1 protocol to communicate with these devices. The number of recommend TL1 active session for the NCS2K devices is not more than 15. If the number of active sessions is more than 15, Cisco Evolved Programmable Network Manager may not able to receive TL1 event from device for any granular or reactive inventory operations. Cisco NCS 4000 series devices, on the other hand, are Cisco IOS-XR devices, and Cisco Evolved Programmable Network Manager uses the SNMP and Telnet/SSH protocols to communicate with these devices.

Before you begin

Check Configure Devices So They Can Be Modeled and Monitored, on page 53 to make sure the Cisco NCS devices are configured correctly.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 Click the + icon above the Network Devices table, then choose **Add Device**.

Step 3 In the **Add Device** dialog box, complete the required fields. Click the **?** icon next to a field for a description of that field.

- Cisco NCS 2000 series and Cisco ONS 15454—Enter TL1 parameters
- Cisco NCS 4000 series—Enter SNMP and Telnet/SSH parameters

Step 4 Click **Verify Credentials** to validate that Cisco Evolved Programmable Network Manager can reach the device.

Step 5 Click **Add** to add the device to Cisco Evolved Programmable Network Manager.

Example: Add a Network Element as an ENE Using Proxy Settings

Messages sent to a particular network element must pass through other NEs in the network. To pass messages, one or more nodes can be a Gateway Network Element (GNE) and connect other NEs in your network. A node becomes a GNE when you establish a TL1 session and enter a command that must be sent to another node. The node that receives the TL1 message from another node for processing is an End-point Network Element (ENE). Messages from an ENE are transmitted through a GNE to other NEs in the network.

Before you begin

Check Configure Devices So They Can Be Modeled and Monitored, on page 53 to make sure your devices are configured correctly.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 Click the + icon above the Network Devices table, then choose **Add Device**.

Step 3 In the **Add Device** dialog box, under **General Parameters**, enter the IP address or the DNS name of the ENE that you want to add. Click the **?** icon next to a field for a description of that field.

Step 4 Under **TL1 Parameters**, enter the primary and secondary proxy IP address for the node that you are using as an ENE.

Note The secondary proxy IP address is optional, and will be activated only in the event of failure of the primary proxy.

Step 5 Click **Verify Credentials** to validate that Cisco EPN Manager can connect to the device.

Step 6 Click **Add** to add the device to Cisco EPN Manager.

Example: Enabling a Single Session on Cisco NCS 2000 Series Devices

Cisco NCS 2000 series devices are TL1-based devices and Cisco EPN Manager uses the TL1 protocol to communicate with these devices. You can edit a newly added device or configure an existing NCS 2000 devices to limit the machine (EMS) account with single session.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 Select a device and then click the Edit icon. The **Edit Device** window appears.

Step 3 To edit a single session on a new device or on existing device, set the following parameters:

a) Check the **Enable Single Session TL1** check box under **TL1 Parameters**.

b) Enter the required parameters.

c) Do one of the following:

- Click **Update** to update the single session settings only on the database.
- Click **Update & Sync** to update both the database and device with the single session settings.

Step 4 (Optional) You can also edit the single session through Bulk Import and Bulk Edit operations.

Note By default, the single session is disabled for the bulk edit. You must check the **Enable Single Session TL1** check box to enable it for all the devices to be imported. Selecting the Bulk Import option might affect the single session flag.

What to do next

To verify the enabled single session

1. Launch the Cisco Transport Controller and select the device for which the single session is enabled.
2. Choose **Provisioning** > **Security** > **Active Logins** to view all the active devices with single sessions. The devices for which the single session is disabled will not be displayed.

Note The credentials check is the only exception while performing the single session task

Establish Strong SSH for Device Communication

Follow this procedure to connect to devices with more secure SSH connection.

Step 1 Connect to the server using SSH and log in as the admin user. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765 for more information.

Step 2 Navigate to `/opt/CSCOlumos/xmp_inventory/xde-home/conf/` directory.

Step 3 Rename the `sampleTransportProperties.xml` file to `transportProperties.xml` in the same directory. This enables Cisco EPN Manager to use stronger ciphers when connecting to the device.

What to do next

Restart Cisco EPN Manager. See Stop and Restart Cisco EPN Manager, on page 769.

Note To revert to the previous connection, rename the `transportProperties.xml` file to `sampleTransportProperties.xml` and restart Cisco EPN Manager.

Add SVO Devices

SVO is a solution to support multi chassis behavior. SVO device can support one NCS2k ROADM and 50 NCS2k OLA instances. With SVO devices, Cisco EPN Manager will move to managed plane provisioning. From 12.0.1, the Cisco EPN Manager will uses the Netconf to communicate with SVO instances.

Before you begin

Check Configure Devices So They Can Be Modeled and Monitored, on page 53 to make sure the Cisco NCS devices are configured correctly.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 Click the + icon above the Network Devices table, then choose **Add Device**.

Step 3 In the **Add Device** dialog box, complete the required fields.

a) Enter the **IP Address** in the **General** section.
b) Select **Netconf Over SSH2** from the **Protocol** drop down list in the **Telnet/SSH** section.
c) Enter the **Username**, **Password**, and **Confirm Password**.
d) Click **Verify Credentials** to validate that Cisco EPN Manager can reach the device.

Step 4 Click **Add** to add the device to Cisco EPN Manager.

If you click on the **Device Name** hyperlink of this device the SVO Nodal craft web UI opens to display and manage the details of this device if SSO is configured. If SSO is not configured, you need to enter the login credentials in the SVO Nodal craft web UI. To enable SSO from Cisco EPN Manager to SVO Nodal craft web UI, see Enable Single Sign-on (SSO) from Cisco EPN Manager to SVO UI , on page 50.

You can also do a bulk import of the devices.

What to do next

- To create and provision OCHCC and OCH-Trail circuits, see Create and Provision an OCH Circuit, on page 529.
- Performance collection must be enabled on the SVO devices to poll and collect the PM data from underlying NCS2K node. It can be enabled or disabled using the CLI Template for one or more devices.

Device 360 View - SVO

The Device 360 view for SVO devices provides the following information.

Information Provided in Device 360 View	Description
General information and tools	Device type, its OS type and version, its last configuration change, and its last inventory collection. Icons convey the status of the device. Using the menus in the pop up window, you can perform these tasks: • Auto-Refresh—For real-time updates of device status and troubleshooting, enable an on-demand refresh by clicking on the Refresh icon. Alternatively, you can also set the auto-refresh interval to 30 seconds, 1 minute, 2 minutes, or 5 minutes from the drop-down list. Auto-Refresh is OFF by default. **Note** The Auto-Refresh setting is applicable only for the currently open 360 view pop up window. If the view is closed and reopened or another view is opened, by default Auto-Refresh is Off. • Open the Device Details page to view details about software image and configuration file management (**View** > **Details**) • Open the Device Configuration page in the SVO Nodal craft UI to perform any configuration changes on the device by choosing **View** > **Chassis View**. • Select a device for a side-by-side comparison with another device on the basis of information such as raised alarms and the current status of circuits, interfaces, and modules (**Actions** menu)—see Compare Device Information and Status, on page 88 • Troubleshoot—Perform a ping or traceroute, launch the Alarm browser, open a Cisco support case, or get information from the Cisco Support Community (**Actions** menu) • Topology—View the network topology and the device's local topology, up to 3 hops (**Actions** menu) • Collect the device's inventory and save it to the database using **Sync Now**, **Sync and Rebuild** (**Actions** menu)
Alarms tab	Current alarms for the device, including their severity, status, and the time they were generated.

Modules tab	Modules that are configured on the device, including their name, type, state, ports, and location.
Interfaces tab	Interfaces that are configured on the device, including status information. You can also launch an Interface 360 view for a specific interface.
Neighbors tab	NEs that are connected to this device through Cisco Discovery Protocol (CDP). If the selected device does not support CDP, this tab is empty. Displayed information includes device type and name, and the local port and device port. To view the neighbors in a pop up topology map, choose **Actions > N Hop Topology** from the top right of the Device 360 view (see View a Device's Local Topology from the Device 360 View, on page 89.
Circuit/VCs tab	Circuit/VC name, type, customer, status, and creation date for each circuit provisioned on the device. You can also launch a Circuit/VC 360 view for specific circuits/VCs.
Civic Location	Geographical information about device's location.
Recent Changes	The last five changes made on the device, classified as: Inventory, Config (Configuration Archive), or SWIM (Software Images). (These are the same types of changes that are displayed when you choose **Inventory** > **Network Audit**.) **Note** If you have logged in as a root user, then you can view all the activities under the Recent Changes tab. If you have logged in as a non-root user, then you can only view the activities performed by you.

You can also view a specific device in the topology map by choosing **Actions** > **Network Topology** (at the top right of the Device 360 view).

SVO UI Overview

Here are the details of the different sections and their respective tabs in SVO:

Table 6: SVO UI Details

Section	Details
SVO Topology	This section shows the topological view of the devices.
Fault Monitoring	This section shows the Alarms, Conditions, History, and Profiles.You can export details of alarms, conditions, and history. You can also load alarm profiles, associate alarms, and manage alarm resources.
Device Configuration	This section allows you to manage the Authorization Groups, Devices, and Diagnostics. You can also configure the IPv4 settings and apply the device settings.

Section	Details
Node Configuration	Here are the details of the action that can be performed in the respective tabs in this section: • Optical Configuration: You can manage the Internal Patch Cords, Connection Verification, Optical Degrees, Fiber Attributes, OSC Terminations, GCC Terminations, Optical Degree Power Monitoring, APC, and measure and export the Span Loss data. • ANS Parameters: You can view export the details for the Amplifier, Interface, Raman Amplifier, and Raman Interface. • Optical Cross Connections: You can view and export the optical cross connection data. • OTDR: You can manage OTDR Provisioning and traces. • XML Configuration: You can select an XML configuration file and load the configuration from it.
SVO Configuration	This section allows you to set up date and time for SVO. You can also retrieve and download SVO and System Logs.
Database	This section shows the database details.
Software Manager	This section allows you to download and manage the SVO and device software packages.
Inventory	This section allows you the view and export the inventory data.
Users Configuration	This section helps you to manage users, manage the SSO configuration and users, and manage the RADIUS configuration.

If required, you can click on the **Device Name** hyperlink of an SVO device, to display the device details in the SVO window. On the Chassis view you can select a card and perform a **Open Card**, **Delete, Soft Reset**, **Hard Reset**, **OBFL**, and **Change Admin State** actions. For the selected card you can select **Open Card** and view the Alarms, Conditions, History, Maintenance, and Performance Details in the respective tabs. You can click on the Provisioning tab to add Pluggable Port Modules, Card Mode, Pluggable Ports, Trail Trace Monitoring, ODU Interfaces, OTU interfaces, Ethernet Interfaces, Optical Channels, Optical Thresholds, G709 Thresholds, FEC Thresholds, UDC, and RMON Thresholds for the selected card. Once done the respective changes will be displayed in the Device 360 and Interface 360 view in EPNM.

Enable Single Sign-on (SSO) from Cisco EPN Manager to SVO UI

To enable Single Sign-on (SSO) from Cisco EPN Manager to SVO UI:

Step 1 Log in to the SVO UI.

Step 2 From the **Menu** navigate to **Access Configuration** and click the **SSO** tab.

Step 3 Under the **SSO Configuration** area, select the **Enable SSO** check box.

Step 4 Enter **IP Address** and **Port** details of the Cisco EPN Manager server from which you wish to cross-launch the SVO UI and click **Apply**.

Step 5 Under **SSO**, click + to add the username. Assign appropriate role to the user and click **Apply**.

Migrating Existing NCS2K-Based Networks

You can migrate the existing NCS2K based networks using the **Optical Circuits/VCs Migrator** window.

You can migrate a maximum of 20 circuits at a time.

Note

- OCH-Trail migration is supported for OTU3, OTU2, OTU2E, OTU4, and OTU4C2.
- OCH-CC migration is support for 100G, 10G, and 40G.

To migrate the existing NCS2K-based networks, carry out these steps:

Before you begin

- NCS2K nodes must be upgraded to 12.3 and equipped with an SVO card.
- Both NCS2K and SVO nodes must be modeled in EPNM and added to different user-defined groups.
- NCS2K and SVO nodes must be in sync.
- Sync both NCS2K and SVO nodes on the EPNM server.
- Move the NCS2K and SVO devices to maintenance state in EPNM.
- Do not modify the circuits set for migration from EPNM.

Step 1 Go to **Inventory > Other** and select **Optical Circuits/VCs Migrator**.

The Optical Circuits/VCs Migrator page appears displaying the list of circuit names that can be migrated.

Step 2 Select the circuit names that you want to migrate.

The migration status of the circuits will be displayed as **Not migrated**.

Step 3 Click **Migrate Circuits**.

Once the migration is done, the migration status of the circuit changes to **Success**. The migrated circuit names will be removed once this page is refreshed.

What to do next

Check the Network Topology page. You will find the migrated circuit's name appearing twice. Check the circuit details in the Circuit/VC 360 view for both the circuits. The migrated circuits will have all the details (alarms, endpoints, history, and related circuit/VCs). The other circuit will indicate the circuit type that is

substituted with the word Legacy and will not have the related details. These devices can be deleted from the Network Devices page. The migrated circuits can be modified and deleted if required. If we model it in two user define groups, you can filter and check the circuits. You will not see duplicate circuits.

How Is Inventory Collected?

After devices are added and discovered, Cisco EPN Manager will collect physical and logical inventory information and save it to the database. The following table describes how inventory collection is triggered.

Inventory Collection Trigger	Description
In response to incoming events	Cisco EPN Manager receives an incoming NE SNMP trap, syslog, or TL1 message that signals a change on the NE. These incoming events include: • Configuration change events that signal a change in the device configuration. These events are normally syslogs or traps. • Other inventory events, such as tunnel up/down, link up/down, module in/out, and so forth. Cisco EPN Manager reacts to these incoming events by collecting NE inventory and state information to make sure that information in its database conforms to that of the NE. Most events trigger granular inventory collection, where Cisco EPN Manager only collects data relevant to the change event; other events will trigger a complete collection (sync) of the NE physical and logical inventory. The data that Cisco EPN Manager collects is determined by information in the incoming event, along with metadata that is defined in Cisco EPN Manager. The metadata in Cisco EPN Manager uses a combination of mechanisms—expedited events, reactive inventory, and granular polling—to fine-tune what is collected. For example, if Cisco EPN Manager receives a GMPLS Tunnel State Change event, it will collect ODU tunnel inventory information to discover midpoints and the Z endpoint of the tunnel.
On demand	Users can perform an immediate inventory collection (called *Sync*) from: • Network Devices page—Select one or more devices (by checking check boxes) and click **Sync**. • Device 360 view—Choose **Actions** > **Sync Now**. See Collect a Device's Inventory Now (Sync), on page 449.
Scheduled (daily)	Normal inventory collection is usually performed overnight. Users with sufficient privileges can check when inventory is collected and the status of collection jobs by choosing **Administration** > **Dashboards** > **Job Dashboard** and choosing **System Jobs** > **Inventory and Discovery Jobs.**

Configure Devices So They Can Be Modeled and Monitored

Note For information on the supported configuration of different device families, see, Cisco Evolved Programmable Network Manager Supported Devices.

Ensure that the device is managed in Cisco EPN Manager with full user privilege (Privileged EXEC mode).

Configure Devices to Forward Events to Cisco EPN Manager

To ensure that Cisco EPN Manager can query devices and receive events and notifications from them, you must configure devices to forward events to the Cisco EPN Manager server. For most devices, this means you must configure the devices to forward SNMP traps and syslogs.

For other devices (such as some optical devices), it means you must configure the devices to forward TL1 messages.

If you have a high availability deployment, you must configure devices to forward events to both the primary and secondary servers (unless you are using a virtual IP address; see Using Virtual IP Addressing With HA, on page 882).

In most cases, you should configure this using the **snmp-server host** command. Refer to the topics in this document that list the pre-requisites for the different device operating systems.

Note For information on the required configuration for enabling granular inventory on devices, see Cisco Evolved Programmable Network Manager Supported Syslogs.

Required Settings—Cisco IOS and IOS-XE Device Operating System

```
snmp-server host
snmp-server community public-cmty RO
snmp-server community private-cmty RW
snmp-server ifindex persist
```

```
logging server_IP
logging on
logging buffered 64000 informational

logging source-interface interface_name
logging trap informational
logging event link-status default
```

Disable domain lookups to avoid delay in Telnet/SSH command response:

```
no ip domain-lookup
```

Enable SSH

```
crypto key generate rsa
ip ssh rsa keypair-name keypair-name
crypto key generate rsa usage-keys label key-label modulus modulus-size
ip ssh version [1 | 2]
```

Setup VTY options:

```
line vty <number of vty>
exec-timeout
session-timeout
transport input ssh (requird only if ssh is used)
transport output ssh (required only if ssh isused)
```

Enable CFM modeling:

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO
```

For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha Password priv des Password
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group

snmp-server group Group v3 priv read v1default write v1default notify v1default
snmp-server group Group v3 priv
snmp-server group Group v3 priv notify epnm read epnm
```

Note

- For the device to work seamlessly in Cisco EPN Manager, the SNMP EngineID generated/configured in the device should be unique in the network.
- For the credentials to work, SNMP users should be re-created if the SNMP EngineID is re-configured in the device.

Configure the cache settings at a global level to improve the SNMP interface response time using the configuration:

```
snmp-server cache
```

Syslogs are used by Cisco EPN Manager for alarm and event management. NTP settings ensure that Cisco EPN Manager receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging Server_IP vrf default severity info [port default]
```

Required Settings—Cisco IOS XR Device Operating System

```
snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server entityindex persist
snmp-server ifindex persist

logging server_IP
logging on
logging buffered <307200-125000000>

logging source-interface interface_name

logging trap informational
logging events level informational
logging events link-status
logging events link-status software-interfaces

no cli whitespace completion
domain ipv4 host server_name server_IP
```

Set up VTY options:

```
line default
exec-timeout 10 0
session-limit 10
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default
```

Telnet and SSH Settings:

```
telnet ipv4 server max-servers no-limit
telnet vrf default ipv4 server max-servers 100
ssh server v2
ssh server rate-limit 60
cinetd rate-limit 60
```

Configure the Netconf and XML agents:

```
xml agent tty
netconf agent tty
```

Monitor device with Virtual IP address :

```
ipv4 virtual address use-as-src-addr
ipv4 virtual address Virtual_IP_Address/Subnet_Mask
```

Enable CFM modeling:

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group
snmp-server group Group v3 priv read v1default write v1default notify v1default
```

Note Alternatively, you can navigate to **Configuration** > **Templates** > **Features & Technologies**. From the Templates tab on the left side, select **CLI Templates** > **System Templates - CLI** and deploy the *Default_Manageability_Config-IOS-XR* template to configure the IOS-XR device settings required for Cisco EPN Manager discovery.

Note

- For the device to work seamlessly in Cisco EPN Manager, the SNMP EngineID generated/configured in the device should be unique in the network.
- For the credentials to work, SNMP users should be re-created if the SNMP EngineID is re-configured in the device.

Configure the following to improve the SNMP interface stats response time:

```
snmp-server ifmib stats cache
```

Configure SNMP traps for virtual interfaces to ensure that link-down scenarios are captured:

```
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression TwoHun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression FourHun*
notification linkupdown
```

Enable SNMP entity field replaceable unit (FRU) control traps:

```
snmp-server traps fru-ctrl
```

Syslogs are used by Cisco EPN Manager for alarm and event management. NTP settings ensure that Cisco EPN Manager receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging server_IP vrf name
```

Enable performance management on all optical data unit (ODU) controllers:

```
controller oduX R/S/I/P
per-mon enable
```

Enable performance management for Tandem Connection Monitoring (TCM):

```
tcm id {1-6}
perf-mon enable
```

To open Cisco Transport Controller (CTC) from Cisco EPN Manager, enable the HTTP/HTTPS server:

```
http server ssl
```

If you plan to use the Configuration Archive, devices must be configured as secured. To configure devices from CTC:

1. Choose **Provisioning** > **Security** > **Access**.
2. Set **EMS Access** to secure.

Note

- Ensure that both the MPLS and K9 packages are installed on the device.
- Install the Cisco IOS XR Manageability Package (MGBL).
- Alternatively, all the above prerequisite can also be applied through CLI Templates. Navigate to **Configuration** > **Templates** > **Features&Technologies**. From the **Templates t**ab on the left pane, select **CLI Templates** > **System Templates-CLI** and deploy the **Default_Manageability_Config template**.
- For more information see, Supported Traps and Supported Syslogs..

Required Settings—Cisco NCS Series Devices

For SR policies, apply the following configuration settings on the selected device:

- Configurations to enable events for policy status logging:

```
segment-routing
traffic-eng
logging policy status
```

- Required Settings—Cisco NCS 4000 Series Devices, on page 57
- Required Settings—Cisco NCS 4200 Series Devices, on page 60

Required Settings—Cisco NCS 4000 Series Devices

Attention Ensure that both the MPLS and K9 packages are installed on the device before completing the following steps.

- Cisco EPN Manager uses SSH to secure communication with Cisco NCS 4000 series devices. To enable SSH, apply the following configuration settings on the device:

```
ssh server v2
ssh server rate-limit 600
```

- In MPLS traffic engineering configuration mode, enable event logging:

```
mpls traffic-eng logging events all
```

- Set the VTY options:

```
line default
exec-timeout 10 0
session-limit 10
session-timeout 100
transport input ssh
transport output ssh
vty-pool default 0 99 line-template default
```

- Configure the LMP link:

```
router-id ipv4 unicast local IP address
```

where *local IP address* is the IP address of the device.

- Configure the Netconf and XML agents:

```
xml agent tty
netconf agent tty
```

- Configure SNMP on the device:

```
snmp-server host server_IP
snmp-server community public RO SystemOwner
snmp-server community private RW SystemOwner
snmp-server ifindex persist
```

You can use either SNMPv2 or SNMPv3:

- For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

- For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server group Group v3 priv notify Group read Group
```

For configuring the polling and configuration view, choose one of the following configuration options:

- SNMPv3 default configuration (used for SNMPv3 polling and viewing of the default configuration):

```
snmp-server group Group v3 priv read v1default write v1default notify v1default
```

- SNMPv3 specific configuration:
  - For SNMPv3 polling only:

```
snmp-server group Group v3 priv
```

  - For viewing configuration for SNMPv3 set, polling, and for traps/informs notifications:

```
snmp-server group Group v3 priv notify epnm read epnm write epnm
```

  - For viewing SNMPv3 - LLDP MIB OID configuration:

```
snmp-server view Group 1.0.8802.1.1.2 included
```

For viewing the LAG link, add the following configuration on device:

```
snmp-server view all 1.0.8802 included
```

Note In the first line, *User* and *Group* are two distinct variables that you must enter values for.

- Configure the stats command to improve the SNMP interface stats response time using the configuration

```
Snmp-server ifmib stats cache
```

- Configure SNMP traps for virtual interfaces to ensure that link-down scenarios are captured:

```
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
```

- Syslogs are used by Cisco EPN Manager for alarm and event management. NTP settings ensure that Cisco EPN Manager receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging server_IP vrf name
```

Note the following:

  - When specifying the time zone, enter the time zone's acronym and its difference (in hours) from Coordinated Universal Time (UTC). For example, to specify the time zone for a device located in Los Angeles, you would enter `clock timezone PDT -7`.
  - Replace *server_IP* with the IP address of the host Cisco EPN Manager is installed on.

- Configure the Virtual IP address:

```
ipv4 virtual address NCS4K_Virtual_IP_Address/Subnet_Mask
ipv4 virtual address use-as-src-addr
```

Note *NCS4K_Virtual_IP_Address* and *Subnet_Mask* are two distinct variables that are separated by a slash. Be sure to enter a value for both of these variables.

- Enable performance management on all optical data unit (ODU) controllers:

```
controller oduX R/S/I/P
per-mon enable
```

- Enable event logging of link status messages for optics controllers of Cisco NCS4000 devices running Cisco IOS release 6.1.42 or later:

```
controller Optics <x/y/z/w>
logging events link-status
```

- Enable performance management for Tandem Connection Monitoring (TCM):

```
tcm id {1-6}
perf-mon enable
```

- Configure the Telnet or SSH rate limit for accepting service requests:
  - For Telnet, set the number of requests that are accepted per *second* (between1-100; the default is 1):

    ```
    cinetd rate-limit 100
    ```

  - For SSH, set the number of requests that are accepted per *minute* (between 1-600; the default is 60):

    ```
    ssh server rate-limit 600
    ```

- To open Cisco Transport Controller (CTC) from Cisco EPN Manager (from a Device 360 view), enable the HTTP/HTTPS server:

```
http server ssl
```

- If you plan to use the Configuration Archive feature, devices must be configured as *secured*. To do this from CTC:
  1. Choose **Provisioning** > **Security** > **Access**
  2. Set EMS Access to **secure**.

- If you notice any performance issues because multiple Cisco NCS 4000 Series devices are sending information simultaneously, increase the number of Telnet sessions per *second*:

```
cinetd rate-limit 100
```

Required Settings—Cisco NCS 4200 Series Devices

- Cisco EPN Manager uses SSH to secure communication with Cisco NCS 4200 series devices. To enable SSH, apply one the following configuration settings on the device:

  - ```
    enable
    configure terminal
    hostname name
    ip domain-name name
    crypto key generate rsa
    ```

  - ```
    enable
    configure terminal
    ip ssh rsa keypair-name keypair-name
    crypto key generate rsa usage-keys label key-label modulus modulus-size
    ip ssh version [1 | 2]
    ```

- Set the VTY options:

```
line vty <#>
exec-timeout
session-timeout
```

```
transport input ssh
transport output ssh
```

- Configure SNMP on the device:

```
snmp-server host server_IP
snmp-server community public RO
snmp-server community private RW
```

You can use either SNMPv2 or SNMPv3:

- For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO
```

- For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha Password priv des  Password
snmp-server view Group 1.3.6 included
snmp-server group Group v3 priv notify Group
```

For configuring the polling and configuration view, choose one of the following configuration options:

- SNMPv3 default configuration (used for SNMPv3 polling and viewing of the default configuration):

```
snmp-server group Group v3 priv read v1default write v1default notify v1default
```

- SNMPv3 specific configuration:
  - For SNMPv3 polling only:

```
snmp-server group Group v3 priv
```

  - For viewing configuration for SNMPv3 set, polling, and for traps/informs notifications:

```
snmp-server group Group v3 priv notify epnm read epnm
```

  - For viewing SNMPv3 - LLDP MIB OID configuration:

```
snmp-server view Group 1.0.8802.1.1.2 included
```

Note In the first line, *User* and *Group* are two distinct variables that you must enter values for.

- Configure the cache settings at a global level to improve the SNMP interface response time using the configuration `Snmp-server cache`
- Syslogs are used by Cisco EPN Manager for alarm and event management. NTP settings ensure that Cisco EPN Manager receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging server_IP vrf default severity info [port default]
mpls traffic-eng logging lsp setups
mpls traffic-eng logging lsp teardowns
```

Note the following:

- When specifying the time zone, enter the time zone's acronym and its difference (in hours) from Coordinated Universal Time (UTC). For example, to specify the time zone for a device located in Los Angeles, you would enter `clock timezone PDT -7`.
- Replace *server_IP* with the IP address of the host Cisco EPN Manager is installed on.

Required Settings—Cisco ASR Series Devices

For SR policies, apply the following configuration settings on the selected device:

- Configurations to enable events for policy status logging:

```
segment-routing
traffic-eng
logging policy status
```

Automatic Push of Required Settings

You can apply mandatory device manageability configurations automatically when a new device (IOS, IOS-XE, and IOS-XR) is added to the inventory. It helps to automatically make the devices manageable by Cisco Evolved Programmable Network Manager, reduces the incident rate of partial collection failures, and removes the need for manually applying the configurations to devices. The required settings for Cisco Evolved Programmable Network Manager device manageability are bundled into pre-configured templates, also known as device manageability templates.

Note Device manageability template overrides the existing configuration, if there exists any.

To automatically deploy the templates to devices, choose **Administration** > **Settings** > **System Settings** > **Inventory** > **Inventory**, and then check the **Enable Device Manageability** check box. By default, this option is enabled. Once this option is enabled, any of the following templates is deployed during device addition, based on the type of device added (for example, if you add an IOS-XR device, then the *AutoDeploy_Manageability_Config-IOS-XR* template is deployed.).

- AutoDeploy_Manageability_Config-IOS
- AutoDeploy_Manageability_Config-IOS-XE
- AutoDeploy_Manageability_Config-IOS-XR

These templates are located in **Configuration** > **Templates** > **Features & Technologies** > **CLI Templates** > **System Templates - CLI**.

Note If the system defined templates are not suitable, you can create a user defined template based on these system templates. Update the new template name under '`/opt/CSCOlumos/conf/ifm/ifm_inventory`' properties file for respective device type. This change will take effect after 5 minutes. Server restart is not required.

Exiting entries in ifm_inventory.properties:

```
ifm.inventory.managebility.prerequisite.ios=AutoDeploy_Manageability_Config-IOS
ifm.inventory.managebility.prerequisite.iosxr=AutoDeploy_Manageability_Config-IOS-XR
ifm.inventory.managebility.prerequisite.iosxe=AutoDeploy_Manageability_Config-IOS-XE
```

User can update the above entries to point to new template names. For example, if user wants to add a template `Updated_AutoDeploy_Manageability_Config-IOS-XR` for IOS-XR device, then entry in file should be updated as:

```
ifm.inventory.managebility.prerequisite.iosxr=Updated_AutoDeploy_Manageability_Config-IOS-XR
```

The **Change Audit Dashboard** (choose **Monitor** > **Tools** > **Change Audit Dashboard**) displays the audit log for each device addition and its corresponding template deployment.

Limitation:

Updating SNMP/CLI timeout also triggers template deployment when the device is not in Completed state.

Required Settings—Cisco ONS Device Operating System

If you plan to use the Configuration Archive feature, devices must be configured as *secured*. You can do this from CTC:

1. From CTC, choose **Provisioning** > **Security** > **Access**.
2. Set EMS Access to secure.

Required Settings—Cisco NCS2K Device

If you plan to use the Configuration Archive feature on NCS2K devices, enable the HTTP/HTTPS server.

Note For the devices where single session is not enabled or applicable, do the following to restrict the number of connections to be used in EPNM:

1. Open **`$XMP_HOME/xmp_inventory/xde-home/inventoryDefaults/onsTL1.def`**
2. Add a new attribute tag as below after the **</test>** tag where **ConnectionCount** must be replaced with actual number (for example: 5).

   *<default attribute="DEVICE_THROTTLING">**ConnectionCount**</default>*

Required Configuration for IPv6 Devices

If you want to access a device that uses IPv6 addresses, configure the IPv6 address and static route on the Cisco EPN Manager server (virtual machine) by performing these steps:

1. Remove the ipv6 address autoconfig from the interface.
2. Configure the IPv6 address on the Cisco EPN Manager server.
3. Add a static route to the Cisco EPN Manager server.

Enable Archive Logging on Devices

Follow these steps to enable archive logging on devices so that granular inventory can be enabled for those devices on Cisco EPN Manager:

For Cisco IOS-XR devices:

```
logging  <epnm server ip>  vrf default severity alerts
logging  <epnm server ip>  vrf default severity critical
logging  <epnm server ip>  vrf default severity error
logging  <epnm server ip>  vrf default severity warning
logging  <epnm server ip>  vrf default severity notifications
logging  <epnm server ip>  vrf default severity info
snmp-server host <epnm server ip>  traps version 2c public
```

For Cisco IOS and IOS-XE devices:

```
logging host <epnm server ip>  transport udp port 514
logging host <epnm server ip>  vrf Mgmt-intf transport udp port 514
snmp-server host <epnm server ip>  traps version 2c public
```

Apply Device Credentials Consistently Using Credential Profiles

Credential profiles are collections of device credentials for SNMP, Telnet/SSH, HTTP, and TL1. When you add devices, you can specify the credential profile the devices should use. This lets you apply credential settings consistently across devices.

If you need to make a credential change, such as changing a device password, you can edit the profile so that the settings are updated across all devices that use that profile.

To view the existing profiles, choose **Inventory > Device Management > Credential Profiles**.

Create a New Credential Profile

Use this procedure to create a new credential profile. You can then use the profile to apply credentials consistently across products, or when you add new devices.

Step 1 Select **Inventory** > **Device Management** > **Credential Profiles**.

Step 2 If an existing credential profile has most of the settings you need, select it and click **Copy**. Otherwise, click **Add**.

Step 3 Enter a profile name and description. If you have many credential profiles, make the name and description as informative as possible because that information will be displayed on the Credential Profiles page.

Step 4 Enter the credentials for the profile. When a device is added or updated using this profile, the content you specify here is applied to the device.

The SNMP read community string is required.

Step 5 Click **Save Changes**.

Apply a New or Changed Profile to Existing Devices

Use this procedure to perform a bulk edit of devices and change the credential profile the devices are associated with. This operation overwrites any existing association between a device and a credential profile. You can also use this operation to synchronize device configurations with the new settings.

Note Make sure the profile's credential settings are correct before following this procedure and selecting **Update and Sync**. That operation will synchronize the devices with the new profile.

Step 1 Configure the credential profile using one of these methods:

- Create a new credential profile by choosing **Inventory** > **Device Management** > **Credential Profiles**, and clicking **Add**.
- Edit an existing profile by choosing **Inventory** > **Device Management** > **Credential Profiles**, selecting the profile, and clicking **Edit**.

Step 2 When you are satisfied with the profile, choose **Inventory** > **Device Management** > **Network Devices**.

Step 3 Filter and select all of the devices you want to change (bulk edit).

Step 4 Click **Edit**, and select the new credential profile from the Credential Profile drop-down list.

Step 5 Save your changes:

- **Update** saves your changes to the Cisco EPN Manager database.
- **Update and Sync** saves your changes to the Cisco EPN Manager database, collects the device's physical and logical inventory, and saves all inventory changes to the Cisco EPN Manager database.

Delete a Credential Profile

This procedure deletes a credential profile from Cisco EPN Manager. If the profile is currently associated with any devices, you must disassociate them from the profile.

Step 1 Check whether any devices are using the profile.

a) Go to **Inventory** > **Device Management** > **Credential Profiles**.
b) Select the credential profile to be deleted.
c) Click **Edit**, and check if any devices are listed on the Device List page. If any devices are listed, make note of them.

Step 2 If required, disassociate devices from the profile.

a) Go to **Inventory** > **Device Management** > **Network Devices**.
b) Filter and select all of the devices you want to change (bulk edit).

c) Click **Edit**, and choose **--Select--** from the Credential Profile drop-down list.
d) Disassociate the devices from the old profile by clicking **OK** in the warning dialog box.

Step 3 Delete the credential profile by choosing **Inventory** > **Device Management** > **Credential Profiles**, selecting the profile, and clicking **Delete**.

Check a Device's Reachability State and Admin Status

Use this procedure to determine whether server can communicate with a device (reachability state) and whether it is managing that device (admin status). The admin status also provides information on whether the device is being successfully managed by the Cisco EPN Manager server.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 Locate your device in the Network Devices table.

a) From the **Show** drop-down list (at the top right of the table), choose **Quick Filter**.
b) Enter the device name (or part of it) in the text box under the **Device Name** column.

Step 3 Check the information in the **Reachability** and **Admin Status** columns. See Device Reachability and Admin States, on page 66 for descriptions of these states.

Device Reachability and Admin States

Device Reachability State—Indicates whether Cisco Evolved Programmable Network Manager can communicate with the device using all configured protocols.

Table 7: Device Reachability State

Icon	Device Reachability State	Description	Troubleshooting
	Reachable	Cisco Evolved Programmable Network Manager can reach the device using SNMP, or the NCS 2K device using ICMP.	—
	Ping reachable	Cisco Evolved Programmable Network Manager can reach the device using Ping, but not via SNMP.	Although ICMP ping is successful, check for all possible reasons why SNMP communication is failing. Check that device SNMP credentials are the same in both the device and in Cisco Evolved Programmable Network Manager, whether SNMP is enabled on the device, or whether the transport network is dropping SNMP packets due to reasons such as mis-configuration, etc. See Change Basic Device Properties, on page 315.

	Unreachable	Cisco Evolved Programmable Network Manager cannot reach the device using Ping.	Verify that the physical device is operational and connected to the network.
	Unknown	Cisco Evolved Programmable Network Manager cannot connect to the device.	Check the device.

Device Admin State—Indicates the configured state of the device (for example, if an administrator has manually shut down a device, as opposed to a device being down because it is not reachable by Ping).

Table 8: Device Admin State

Device Admin State	Description	Troubleshooting
Managed	Cisco Evolved Programmable Network Manager is actively monitoring the device.	Not Applicable.
Maintenance	Cisco Evolved Programmable Network Manager is checking the device for reachability but is not processing traps, syslogs, or TL1 messages.	To move a device back to Managed state, see Move a Device To and From Maintenance State, on page 68.
Unmanaged	Cisco Evolved Programmable Network Manager is not monitoring the device.	In the Network Devices table, locate the device and click the "i" icon next to the data in the **Last Inventory Collection Status** column. The popup window will provide details and troubleshooting tips. Typical reasons for collection problems are: • Device SNMP credentials are incorrect. • The Cisco Evolved Programmable Network Manager deployment has exceeded the number of devices allowed by its license. • A device is enabled for switch path tracing only. If a device type is not supported, its Device Type will be **Unknown**. You can check if support for that device type is available from Cisco.com by choosing **Administration** > **Licenses and Software Updates** > **Software Update** and then clicking **Check for Updates**.
Unknown	Cisco Evolved Programmable Network Manager cannot connect to the device.	Check the device.

Move a Device To and From Maintenance State

When a device's admin status is changed to Maintenance, Cisco Evolved Programmable Network Manager will neither poll the device for inventory changes, nor will it process any traps or syslogs that are generated by the device. However, Cisco Evolved Programmable Network Manager will continue to maintain existing links and check the device for reachability.

See Device Reachability and Admin States, on page 66 for a list of all admin states and their icons.

Step 1 From the Network Devices table, choose **Admin State** > **Set to Maintenance State**.

Step 2 To return the device to the fully managed state, choose **Admin State** > **Set to Managed State**.

Note You can also schedule devices to maintenance on specific date and time and return them back to Managed state on specific date and time using **Schedule Maintenance State** and **Schedule Managed State** options.

Move a Line Card To and From Maintenance State

When the status of a line card is changed to Maintenance, the Cisco EPN Manager will not process any traps, alarms, or syslogs that are generated by that line card. However, the Cisco EPN Manager will continue to maintain existing links and check the line card for reachability.

To move a line card to and from the maintenance state:

Step 1 Open the Chassis Explorer (see View and Manage Devices Using the Chassis View, on page 92) for the device and choose **Launch Configuration**. Select the line card that you want to move and click the ***i*** icon.

Step 2 Choose **Set to Maintenance**. You can also check the line card status here.

Step 3 To move the line card to fully managed state, follow the steps given above and choose **Set to Managed State** in the menu.

Note Moving a line card to **Maintenance State** or **Managed State** will also move the ports associated with that line card.

Move a Port To and From Maintenance State

When the status of a port is changed to Maintenance, the Cisco EPN Manager will not process any traps, alarms, or syslogs that are generated by that port. However, the Cisco EPN Manager will continue to maintain existing links and check the port for reachability.

To move a port to and from the maintenance state:

Step 1 Open the Interface 360 window (see Get a Quick Look at a Device Interface: Interface 360 View, on page 103) and choose **Actions** > **Set to Maintenance**.

Step 2 To move the port to fully managed state, follow the steps given above and choose **Set to Managed** in the menu.

Validate Added Devices and Troubleshoot Problems

To monitor the discovery process, follow these steps:

Step 1 To check the discovery process, choose **Inventory** > **Device Management** > **Discovery**.

Step 2 Expand the job instance to view its details, then click each of the following tabs to view details about that device's discovery:

- Reachable—Devices that were reached using ICMP. Devices may be reachable, but not modeled, this may happen due to various reasons as discussed in Add Devices Using Discovery, on page 38. Check the information in this tab for any failures.
- Filtered—Devices that were filtered out according to the customized discovery settings.
- Ping Reachable—Devices that were reachable by ICMP ping but could not be communicated using SNMP. This might be due to multiple reasons: invalid SNMP credentials, SNMP not enabled in device, network dropping SNMP packets, etc.
- Unreachable—Devices that did not respond to ICMP ping, with the failure reason.
- Unknown—Cisco Evolved Programmable Network Manager cannot connect to the device by ICMP or SNMP.

Note For devices that use the TL1 protocol, make sure that node names do not contain spaces. Otherwise, you will see a connectivity failure.

Step 3 To verify that devices were successfully added to Cisco Evolved Programmable Network Manager, choose **Inventory** > **Device Management** > **Network Devices**. Then:

- Verify that the devices you have added appear in the list. Click a device name to view the device configurations and the software images that Cisco Evolved Programmable Network Manager collected from the devices.
- View details about the information that was collected from the device by hovering your mouse cursor over the Inventory Collection Status field and clicking the icon that appears.
- Check the device's Reachability and Admin Status columns. See Device Reachability and Admin States, on page 66.

If you need to edit the device information, see Change Basic Device Properties, on page 315.

To verify that Cisco EPN Manager supports a device, refer to Cisco Evolved Programmable Network Manager.

To verify that Cisco Evolved Programmable Network Manager supports a device, click the Settings icon (⚙), then choose **Supported Devices**.

Find Devices With Inventory Collection or Discovery Problems

Use the quick filter to locate devices that have discovery or collection problems.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices** to open the Network Devices page.

Step 2 Make sure **Quick Filter** is listed in the **Show** drop-down at the top left of the table.

Step 3 Place your cursor in the quick filter field below the **Last Inventory Collection Status** and select a status from the drop-down list that is displayed. The devices are filtered according to that status. For troubleshooting steps, see Validate Added Devices and Troubleshoot Problems, on page 69.

Retry Job for Device Modeling

During device discovery, certain transient conditions can cause a device to have the **Last Inventory Collection Status** value as *Completed with Warning*. In such cases, the failed features of these devices will be automatically recovered using the **Failed Feature Sync**.

Note *Completed with Warning* state is indicated when a device moves to *Completed* state and usable from the Cisco EPN Manager, but has certain features that have failed and are unusable. These failed features are listed and can be recovered by the user by performing the recommended action.

Note

- The **Failed Feature Sync** job will be used only for devices with *Completed with Warning* status, for certain recoverable failures (for example, a timeout error). Permanent or system-based errors (for example, user authentication error or unknown error) cannot be autorecovered. For more information on the error scenarios, please contact the administration team.
- The **Failed Feature Sync** job works only in the Cisco EPN Manager 3.0 and later versions. For devices that were already in *Completed with Warning* state in previous versions of Cisco EPN Manager and upgraded to 3.0 or later version, user must perform a manual resync of the device before enabling the **Failed Feature Sync** job. As an alternative to manual resync, user can also wait for the daily sync job where the resync will automatically happen. For more information, see Switch Inventory job in System Jobs, on page 781.

The **Failed Feature Sync** job (Go to **Administration** > **Dashboard** > **Job Dashboard**. In the left sidebar, choose **System Jobs** > **Inventory And Discovery Jobs**) is enabled by default. The default job interval (1 hour) can be edited using the **Edit Schedule** option, though it is not recommended to run the job at a reduced interval, unless in case of emergency.

Note If you have more number of devices with *Completed with Warning* status, it is recommended to run the **Failed Feature Sync** job as least often as possible.

Alternately, Cisco EPN Manager provides additional instructions for devices in *Completed with Warning* state that can be followed by the user to resolve failures and move the device to the *Completed* state. In the Network Devices table, locate the device and click the *i* icon next to the data in the **Last Inventory Collection Status** column. The pop-up window provides details and troubleshooting tips (Failures, Impact, Possible Causes, and Recommended Actions). After user performs the recommended actions, the device can be moved to *Completed* state through a manual sync (applicable for errors such as Wrong CLI credentials), or automatically recovered in the next iteration of the **Failed Feature Sync** job.

Here are some of the *Completed with Warning* scenarios and the corresponding recommended actions:

Table 9: Completed with Warning state scenarios

Possible Cause	Recommended Action
Connection to the device failed	Verify that the device accepts incoming CLI/ SNMP connections and retry.
Connection to the device is closed	Verify that the device accepts incoming CLI/ SNMP connections and retry.
Data cap exceeded	Collection Error: Please contact the administrator with inventory logs.
Unexpected condition in the TL1 protocol	Verify that the device accepts incoming TL1 connections and retry.
General unexpected condition in the HTTP protocol	Verify that the device accepts incoming HTTP connections and retry.
Error retrieving from NETCONF/XML	Verify that NETCONF/XML is configured and retry.
NETCONF reported an RPC error	Collection Error: Please contact the administrator with inventory logs.
Error in the CLI_SESSION_SCRIPT document	Verify that the device can accept a new CLI session and retry.
A pattern was matched indicating an error during session setup or tear down	Verify that the device can accept a new CLI session and retry.
Device not reachable	Please contact the administrator with inventory logs.
Failsafe timeout occurred when trying to communicate with the device	Verify device responsiveness and load.
A timeout occurred when trying to communicate with the device	Verify that the timeouts that are configured on the device do not stop CLI connections and retry. Also, check the maximum number of active SSH connections that are configured on the device.
No response for SNMP get request	Verify that the device can accept incoming SNMP requests and retry.
Failed to perform SNMP get request	Verify that the device can accept incoming SNMP requests and retry.

Possible Cause	Recommended Action
Response error for SNMP get request	Verify that the device can accept incoming SNMP requests and retry.

Export Device Information to a CSV File

When you export the device list to a file, all device information is exported into a CSV file. The file is then compressed and encrypted using a password you select. The exported file contains information about the device's SNMP credentials, CLI settings, device groups, and geographical coordinates. The exported file includes device credentials but does not include credential profiles.

Caution Exercise caution while using the CSV file as it lists all credentials for the exported devices. You should ensure that only users with special privileges can perform a device export.

Cisco Evolved Programmable Network Manager supports ZipCrypto encryption method to open the exported file using operating system default zip utility. To enable ZipCrypto encryption method, choose **Administration** > **Settings** > **System Settings** > **Inventory** > **Inventory**, and then check the **Enable ZipCrypto encryption for 'Export Device'** check box. By default, this option is disabled.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 Select the devices that you want to export, then click **Export Device** (or click  and choose **Export Device**).

Step 3 In the **Export Device** dialog box, add and confirm a password that will be used to encrypt the exported CSV file. Users will need to supply this password to open the exported file. Optionally, enter the Export File Name. Depending on your browser configuration, you can open or save the compressed file.

Step 4 Click **Export**.

Note You can open the file only if ZipCrypto encryption is enabled.

Create Groups of Devices for Easier Management and Configuration

- How Groups Work, on page 73
- Create User-Defined Device Groups, on page 76
- Create Location Groups, on page 77
- Create Port Groups, on page 79
- Make Copies of Groups, on page 79

- Delete Groups, on page 80

Organizing your devices into logical groupings simplifies device management, monitoring, and configuration. As you can apply operations to groups, grouping saves time and ensures that configuration settings are applied consistently across your network. In smaller deployments where all devices can be configured with the same settings, you may only need to create one general device group. The grouping mechanism also supports subgroups. You will see these groups in many of the Cisco EPN Manager GUI windows.

When a device is added to Cisco EPN Manager, it is assigned to a location group named **Unassigned**. If you are managing a large number of devices, be sure to move devices into other groups so that the Unassigned Group membership does not become too large.

How Groups Work

Groups are logical containers for network elements, such as devices and ports. You can create groups that are specific to your deployment—for example, by device type or location. You can set up a group so that new devices are automatically added if they match your criteria, or you may want to add devices manually.

For information on the specific types of groups, see the related topics Network Device Groups, on page 73 and Port Groups, on page 74.

For information on how elements are added to groups, see How Elements Are Added to Groups: Dynamic, Manual, and Mixed Groups, on page 75.

Network Device Groups

The following table lists the supported types of network device groups. The device groups can be accessed from the Inventory.

Network Device Group Type	Membership Criteria	Can Be Created or Edited By Users?
Device Type	Devices are grouped by family (for example, Optical Networking, Routers, Switches and Hubs, and so forth). Under each device family, devices are further grouped by series. New devices are automatically assigned to the appropriate family and series groups. For example, a Cisco ASR 9006 would belong to Routers (family) and Cisco ASR 9000 Series Aggregation Services Routers (series). Note the following: • You cannot create a device type group; these are dynamic groups that are system-defined. Instead, use device criteria to create a user-defined group and give it an appropriate device type name. • Device type groups are not displayed in Network Topology maps.	No

Location	Location groups allow you to group devices by location. You can create a hierarchy of location groups(such as theater, country, region, campus, building, and floor) by adding devices manually or by adding devices dynamically. A device should appear in one location group only, though a higher level "parent" group will also contain that device. By default, the top location of the hierarchy is the **All Locations** group. All devices that have not been assigned to a location appear under the Unassigned group under All Locations.	Yes
User Defined	Devices are grouped by a customizable combination of device and location criteria. You can customize group names and use whatever device and location criteria you need.	Yes

Import Location Groups

From the Network Device Groups page, you can import location groups using CSV file. To import a location group using a CSV file that lists all attributes of the group that you want to add into Cisco Evolved Programmable Network Manager:

Step 1 Choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 Click the **Import Groups** button. The **Import Groups** dialog opens.

Step 3 Download the sample template by clicking **here** at the bottom of the displayed dialog. Create a CSV file and enter group name/parent hierarchy/location preference/physical address/latitude/longitude details using the format and information in the template as a guide. Save the CSV file.

Step 4 Click **Browse** in the **Import Groups** dialog, and select the CSV file that contains the group that you want to import.

Step 5 Choose **Administration** > **Dashboards** > **Job Dashboard** and click **Import Groups** to view the status of the job.

Export Location Groups

To export the location group information as a CSV file:

Step 1 Choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 Click the **Export Groups** button. The **Export Groups** dialog opens.

Step 3 Save the CSV file at the desired location. The CSV file provides details such as group name, parent hierarchy, location preference, physical address, latitude, and longitude.

Port Groups

The following table lists the supported types of port groups.

Port Group Type	Membership Criteria	Can be created or edited by users?

Port Type	Grouped by port type, speed, name, or description. Ports on new devices are automatically assigned to the appropriate port group. You cannot create Port Type groups. Instead, use device criteria to create a user-defined group, and create subgroups under the user-defined group.	No; instead create a User Defined Group
System Defined	Grouped by port usage or state. Ports on new devices are automatically assigned to the appropriate port group. Wireless and Data Center devices use the other System Defined port groups: AVC Configured Interfaces, UCS Interfaces, UCS Uplink Interfaces, WAN Interfaces, and so forth. You cannot create System Defined Port groups. Instead, use device criteria to create a user-defined group, and create subgroups under the user-defined group. **Note** As the WAN Interfaces is a static group, automatic port addition is not applicable. Hence, you must add the ports manually to the group.	No; instead create a User Defined Group
User Defined	Grouped by a customizable combination of port criteria, and you can name the group. If the group is dynamic and a port matches the criteria, it is added to the group.	Yes

How Elements Are Added to Groups: Dynamic, Manual, and Mixed Groups

How elements are added to a group depends on whether the group is dynamic, manual, or mixed.

Method for Adding Devices	Description
Dynamic	Cisco Evolved Programmable Network Manager automatically adds a new element to the group if the element meets the group criteria. While there is no limit to the number of rules that you can specify, the performance for updates may be negatively impacted as you add more rules.
Manual	Users add the elements manually when creating the group or by editing the group.
Mixed	Elements are added through a combination of dynamic rules and manual additions.

The device inheritance in parent-child user defined and location groups are as follows:

- User Defined Group—When you create a child group:
  - If the parent and child groups are both dynamic, the child group can only access devices that are in the parent group.
  - If the parent group is static and the child group is dynamic, the child group can access devices that are outside of the parent group.
  - If the parent and child groups are dynamic and static, the child group "inherits” devices from the parent device group.

- Location Group—The parent group inherits the child group devices.

Groups and Virtual Domains

While groups are logical containers for elements, access to the elements is controlled by virtual domains. This example shows the relationship between groups and virtual domains.

- A group named **SanJoseDevices** contains 100 devices.
- A virtual domain named **NorthernCalifornia** contains 400 devices. Those devices are from various groups and include 20 devices from the **SanJoseDevices** group.

Users with access to the **NorthernCalifornia** virtual domain will be able to access the 20 devices from the **SanJoseDevices** group, but not the other 80 devices in the group. For more details, see Create Virtual Domains to Control User Access to Devices, on page 815.

Create User-Defined Device Groups

To create a new device type group, use the user-defined group mechanism. You must use this mechanism because device type groups are a special category that is used throughout Cisco Evolved Programmable Network Manager. The groups that you create appear in the **User Defined** category.

Note Cisco ASR satellites can only belong to location groups. For more information, see Satellite Considerations in Cisco Evolved Programmable Network Manager, on page 270.

To create a new group, complete the following procedure:

Step 1 Choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 In the **Device Groups** pane, click the **+** (**Add**) icon and then choose **Create User Defined Group**.

Step 3 Enter the group's name and description. If other user-defined device type groups exist, you can set one as the parent group by choosing it from the **Parent Group** drop-down list. If you do not select a parent group, the new group resides in the **User-Defined** folder (by default).

Step 4 Add devices to the new group:

If you want to add devices that meet your criteria automatically, enter the criteria in the **Add Devices Dynamically** area. To group devices that fall within a specific range of IP addresses, enter that range in square brackets. For example, you can specify the following:

- IPv4-10.[101-155].[1-255].[1-255] and 10.126.170.[1-180]
- IPv6-2014::5217:[0000-ffff]:fe22:[1e40-1f41]

Note While there is no limit on the number of rules you can specify for a dynamic group, group update performance could become slower as the number of rules increases.

If you want to add devices manually, do the following:

a. Expand the **Add Devices Manually** area and then click **Add**.

b. In the **Add Devices** dialog box, check the check boxes for the devices you want to add, then click **Add**.

Step 5 Click the **Preview** tab to see the members of your group.

Step 6 Click **Save**.

The new device group appears in the folder that you selected in Step 3.

Note The dynamically added device group cannot be deleted after its creation. If you want to add and define devices manually, then you have to delete the dynamically created device group and create a new device group.

Note You can also create device groups by navigating to **Inventory** > **Device Management** > **Configuration Archive** > **Archives** > **Create Group**.

Create Location Groups

Note Cisco ASR satellites can only belong to Location Groups. For more information, see Satellite Considerations in Cisco Evolved Programmable Network Manager, on page 270.

To create a location group, follow these steps:

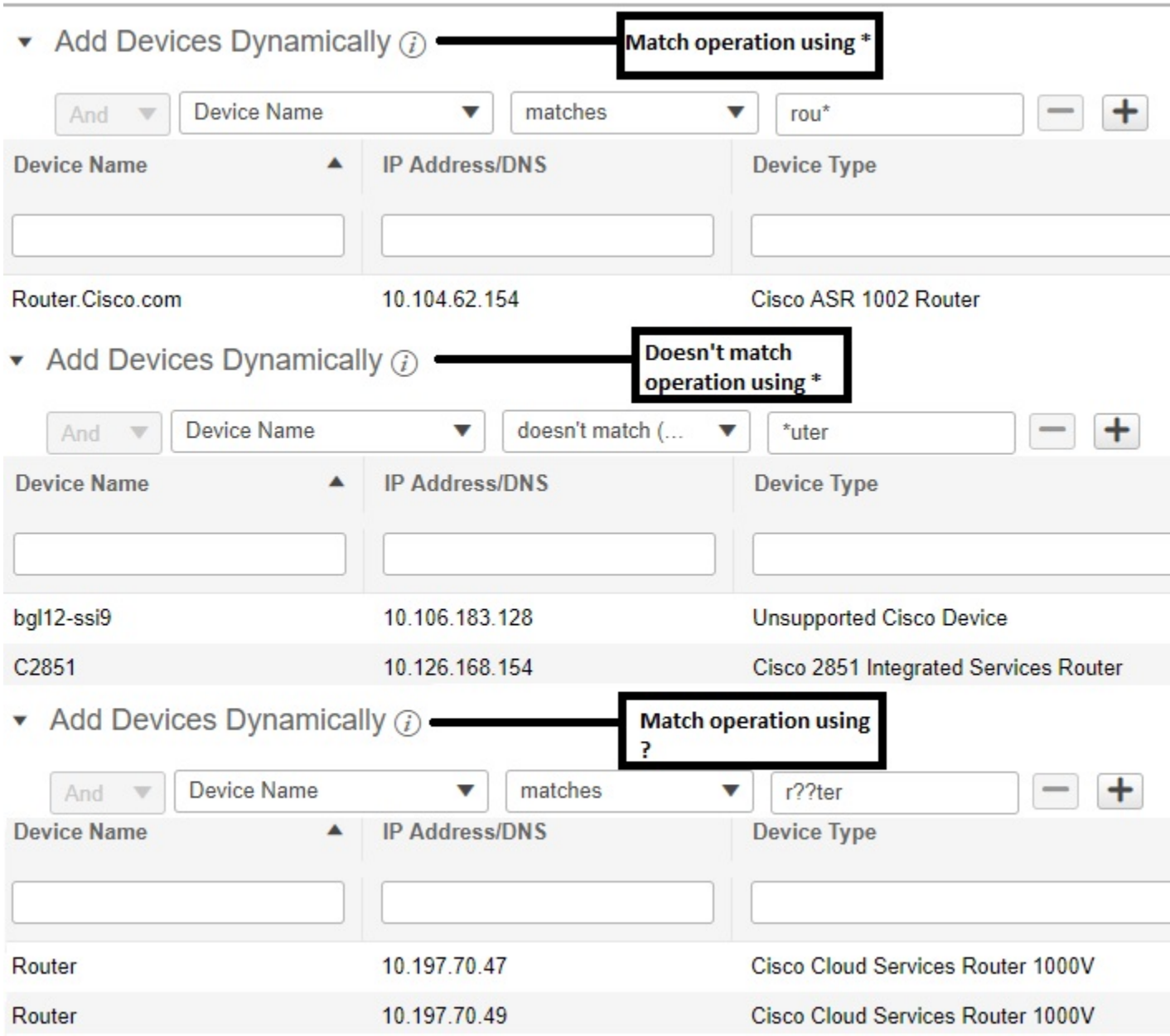
Step 1 Choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 In the **Device Groups** pane on the left, click the **Add** icon, then choose **Create Location Group**.

Step 3 Enter the name and description, and choose a group from the **Parent Group** drop-down list. By default, the group will be an All Locations subgroup (that is, displayed under the **All Locations** folder).

Step 4 If you are creating a device group based on geographical location, for example, all devices located in a building at a specific address, select the Geographical Location check box and specify the GPS coordinates of the group or click the **View Map** link and click on the required location in the map. The GPS coordinates will be populated automatically in this case. Note that location groups defined with a geographic location are represented by a group icon in the geo map. The devices you add to the group will inherit the GPS coordinates of the group. See Device Groups in the Geo Map, on page 205 for more information. Note that if geographical location is the primary reason for grouping a set of devices, it is recommended that the devices you add to the group do not have their own GPS coordinates that are different from the group's.

Step 5 If you want devices to be added automatically if they meet certain criteria, enter the criteria in the **Add Device Dynamically** area. Otherwise, leave this area blank.



While there is no limit on the number of rules that you can specify for a dynamic group, as the number of rules increases, the group update performance could become slower.

Step 6 If you want to add devices manually:

a) Under **Add Devices Manually**, click **Add**.

b) In the **Add Devices** dialog box, locate devices you want to add, then click **Add**.

Step 7 Click the **Preview** tab to see the group members.

Step 8 Click **Save**, and the new location group appears under the folder you selected in Step 3 (**All Locations**, by default).

launch the Maps GUI. click building.

When you edit a location group, you may change the group type if the following conditions are met:

- The group type is Default.
- The group does not have any subgroups.

Create Port Groups

To create a port group, follow these steps:

Step 1 Choose **Inventory** > **Group Management** > **Port Groups**.

Step 2 From **Port Groups** > **User Defined**, hover your cursor over the "i" icon next to **User Defined** and click **Add SubGroup** from the popup window.

Step 3 Enter the name and description, and choose a group from the **Parent Group** drop-down list. By default, the port group will be under the **User Defined** folder.

Step 4 Choose the devices a port must belong to in order to be added to the group. From the **Device Selection** drop-down list, you can select:

- **Device**—To choose devices from a flat list of all devices.
- **Device Group**—To choose device groups (Device Type, Location, and User Defined groups are listed).

Step 5 If you want ports to be added automatically if they meet your criteria, enter the criteria in the **Add Ports Dynamically** area. Otherwise, leave this area blank.

While there is no limit on the number of rules that you can specify for a dynamic group, the group update performance could become slower as the number of rules increases.

Step 6 If you want to add devices manually:

a) Under **Add Ports Manually**, click **Add**.

b) In the **Add Ports dialog** box, locate devices you want to add, then click **Add**.

Step 7 Click the **Preview** tab to see the group members.

Step 8 Click **Save**, and the new port group appears under the folder you selected in Step 3 (**User Defined**, by default).

Make Copies of Groups

When you create a duplicate of a group, Cisco Evolved Programmable Network Manager names the group **CopyOf***group-name* by default. You can change the name, if required.

To duplicate a group follow these steps:

Step 1 Choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 Choose the group from the Device Groups pane on the left.

Step 3 Locate the device group you want to copy, then click the "i" icon next to it to open the pop-up window.

Step 4 Click **Duplicate Group** (do not make any changes yet) and click **Save**. Cisco Evolved Programmable Network Manager creates a new group called **CopyOf***group-name*.

Step 5 Configure your group as described in Create User-Defined Device Groups, on page 76 and Create Location Groups, on page 77.

Step 6 Verify your group settings by clicking the **Preview** tab and examining the group members.

Step 7 Click **Save** to save the group.

Delete Groups

Step 1 Choose **Inventory** > **Group Management** > **Network Device Groups**.

Step 2 Locate the device group you want to delete in the Device Groups pane on the left, then click the "i" icon next to it to open the pop-up window.

Step 3 Click **Delete Group** and click **OK**.

Delete Devices

When you delete a device, Cisco Evolved Programmable Network Manager will no longer model or monitor it.

Before you begin

If a device has services on it that were provisioned using Cisco Evolved Programmable Network Manager, you must delete those services before deleting the device. However, you will be permitted to delete devices that have discovered or provisioned services on it (that is, services that were not created by Cisco Evolved Programmable Network Manager). To find out which services are on a device, use the Device 360 view; see View a Specific Device's Circuits/VCs, on page 637.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices** to open the Network Devices page.

Step 2 Locate the device you want to delete. For example, navigate through the Device Groups list, or enter the text in the Quick Filter boxes.

Step 3 Select the device and click the **Delete Device** icon.

Replace an Existing Network Element

To replace an existing network element with a new network element which is exactly the old device:

Step 1 Choose **Inventory** > **Device Management** > **Configuration Archive** and take the configuration backup for the device that needs to be replaced when it is in the completed state.

Step 2 Choose **Inventory** > **Device Management** > **Network Devices** and change the device state to **Maintenance** for the device that needs to be replaced.

Step 3 Replace the network element with the same hardware, including the RP and line cards which were installed in the same slots as of the old hardware.

Step 4 Reconnect the new hardware to the management port in the same way as the old hardware was connected.

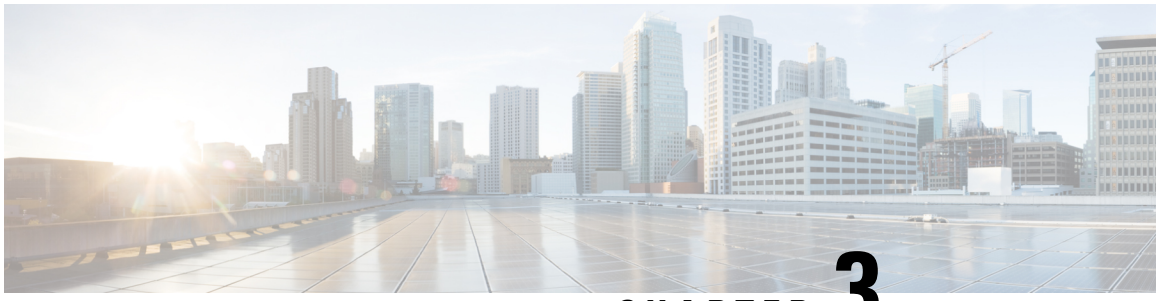
Step 5 Configure the basic management configurations on the new device same as of old device. For example, mangement IP, subnet, hostname, and so on.

Step 6 Choose **Inventory** > **Device Management** > **Configuration Archive** and **Roll Back** the configuration backup taken from the old device on the new device.

Step 7 On the **Network Devices** page, change the device state to **Managed** and wait till the status changes to **Completed**.

What to do next

Make sure that all the basic device settings, services , performance and fault data are intact and the new configuration is successful.



CHAPTER 3

View Device Details

The following topics explain how to get more information about your network devices. You can also generate a variety of device reports that provide hardware and software details, CPU and memory utilization, general device health, and so forth. For information on these reports, see Device Reports, on page 291. For information on inventory collection, see How Is Inventory Collected?, on page 52.

Find Devices

The quickest way to find a device is to use the quick search text boxes displayed at the top of the Network Devices table (**Inventory > Device Management > Network Devices**). You can enter partial strings for a device name, IP address, or software version, or choose from the values for reachability, admin status, and inventory collection. If user defined fields have been created, you can also search by user defined field values. Devices are also organized into device groups, which you can view by choosing **Inventory > Device Management > Network Devices** and selecting a device type from the **Device Group** list.

Get Basic Device Information: Device 360 View

The Device 360 view is a pop-up window that provides quick information about a device, its inventory, and status. This includes device alarms, modules, interfaces, neighbors, memory utilization, CPU utilization, and chassis.

To launch a Device 360 view:

- Click the ***i*** icon next to an IP address in almost any device table.
- From the network topology, click a device in an expanded group, then click **View 360**.

The Device 360 view provides general device and performance information at the top of the view. The information displayed depends on the device type and configuration.

For SVO devices, see Device 360 View - SVO , on page 48.

Information Provided in Device 360 View	Description

General information and tools	

Device type, OS type and version, last configuration change, memory utilization, CPU utilization, and last inventory collection. Icons convey the status of the device.

Note

- If you have opened the Device 360 view for a Cisco NCS 6000 series device that houses a Secure Domain Router (SDR), the SDR's name is also displayed.
- If you have opened the Device 360 view for a Cisco Catalyst 6500 series device with dual and quad-supervisor Virtual Switching System (VSS), the device's redundancy state, switch mode, and operational redundancy mode are also displayed.

Using the menus in the pop-up window, you can also perform these tasks:

- Auto-Refresh—For real-time updates of the device status and troubleshooting, enable an on-demand refresh by clicking the Refresh icon. Alternatively, you can set the autorefresh interval to 30 seconds, 1 minute, 2 minutes, or 5 minutes from the drop-down list. Auto-Refresh is OFF by default.

  Note The Auto-Refresh setting is applicable only for the open 360 view pop-up window. If the view is closed and reopened, or another view is opened, by default Auto-Refresh turns Off.

- Troubleshoot—Perform a ping or traceroute, launch the alarm browser, open a Cisco support case, or get information from the Cisco Support Community (**Actions** menu).
- Performance—Check device CPU and memory (**View** > **Performance Graphs**).
- Topology—View the network topology and device's local topology, up to three hops (**Actions** > > **Network Topology** menu).
- Open the **Device Console** to enter commands you want to run (**Actions** > **Device Console**).
- Collect the device's inventory and save it to the database using **Actions** > **Sync Now**.
- Open an HTTP, HTTPS, SSH, or Telnet session with the device (**Actions** > **Connect To Device**).
- Launch Cisco Transport Controller for optical devices (**Actions** menu).
- Enables you to resync the condition of the selected Cisco NCS 2000 series device with severity NA/NR using **Resync Conditions** (**Actions** menu).
- Open the Device Details page to view the details about software image and configuration file management, and use the device's Chassis View (by clicking the device IP address hyperlink or choosing **View** > **Chassis View**).

	• Open the Configuration page to perform any configuration changes on the device, without navigating from the Device 360 page. Choose **View** > **Configuration**. **Note** This option is available on devices where configuration changes can be performed. For example, Cisco NCS 2000 series devices. • Select a device for a side-by-side comparison with another device based on information such as raised alarms and status of circuits, interfaces, and modules (**Actions** > **Add to Compare**)—see Compare Device Information and Status. • Click **Device OAM** in the **Actions** menu to do a ping test or traceroute between two devices. In the **Device OAM Commands** window, enter the **Destination IP**. Specifying the **Source IP** is optional. From the **Actions** drop-down list, you can either choose a ping test or traceroute.
Performance Graphs	Charts reflecting various aspects of the device performance. If a device has multiple memory pools, the Device 360 view displays the average utilization for all the memory pools. If you want to see information about individual memory pools, use the memory utilization dashlets in the Network Summary dashboard. See Network Summary Dashboard Overview.
Alarms	Current alarms for the device, including their severity, status, and the time they were generated. Depending on the alarm source, you can also launch other 360 views from this tab.
Modules	Modules that are configured on the device, including their name, type, state, ports, and location.
Interfaces	Interfaces that are configured on the device, including status information. You can also launch an Interface 360 view for a specific interface.
Neighbors	NEs that are connected to this device through Cisco Discovery Protocol (CDP). If the selected device does not support CDP, this tab is empty. Displayed information includes device type and name, and local and device ports. To view the neighbors in a pop up topology map, choose **Actions** > **N Hop Topology** (see View a Device's Local Topology from the Device 360 View, on page 89). **Note** This option is not available for Cisco NCS 1010 devices.
Circuit/VCs	Circuit/VC name, type, customer, status, and creation date for each circuit provisioned on the device. You can also launch a Circuit/VC 360 view for specific circuits/VCs. **Note** This option is not available for Cisco NCS 1010 devices.
Satellites tab	For Cisco ASR 9000 series devices in a cluster configuration, this tab lists the satellite's name, type, description, status, IP address, and MAC address. You can also launch a Satellite 360 view for a specific satellite.
Civic Location	Geographical information about device's location.

Recent Changes	The last five changes made on the device, classified as: Inventory, Config (Configuration Archive), or SWIM (Software Images). **Note** If you have logged in as a root user, then you can view all the activities under the Recent Changes tab. If you have logged in as a non-root user, then you can only view the activities you performed.
SRRGs	Lists the Shared Risk Resource Groups (SRRGs) assigned to the device. Click this tab's **?** (**help**) icon to view its legend. For more information about SRRGs, see Manage Shared Risk Resource Groups (SRRGs) in the Geo Map. **Note** This option is not available for Cisco NCS 1010 devices.

You can also view a specific device in the topology map by choosing **Actions** > **Network Topology**.

Compare Device Information and Status

From the **Comparison View** page, you can perform a side-by-side comparison of multiple devices, viewing information such as raised alarms, the status of modules, interfaces, and circuits on those devices, and a summary of recent changes that have been made. To compare devices, do the following:

Step 1 Choose one of the following to open the **Network Devices** page:

- **Monitor** > **Managed Elements** > **Network Devices**
- **Inventory** > **Device Management** > **Network Devices**

Step 2 For each device you want to compare:

a) Open its Device 360 view by clicking the *i* (**information**) icon in the **IP Address** column.

b) Choose **Actions** > **Add to Compare**.

The device you selected is displayed at the bottom of the page. You can select a maximum of 4 devices.

Step 3 Click **Compare**.

The **Comparison View** page opens.

Step 4 From the drop-down list at the top of the view, specify whether the view will show all available information or just the information that is unique to each device.

Step 5 Click **Customize View**, check the check box for the categories you want the view to display, and then click **Save**.

By default, all of the categories are selected.

Step 6 Scroll down the page to view the information provided for each category you selected.

Note the following:

- The **Comparison View** only displays information for two devices at a time. If you selected more than two, you will need to toggle to the devices that are not currently displayed.
- To reorder the devices you have selected, click **Rearrange** at the top right of the page.

- Each device's **View** and **Actions** menu is identical to the ones provided in their Device 360 view. If you select an option, the corresponding page opens.
- You can minimize and maximize the categories displayed, as needed.
- The **Comparison View** is also available for circuits and VCs, interfaces, and links. Whenever you select any of these elements from their respective 360 view for comparison, they are displayed in the corresponding tab. This allows you to switch between element types, as needed.
- When you are done comparing devices, click **Back** at the top right of the page and then click **Clear All Items** at bottom of the page. If tabs for other element types are still displayed, you will need to clear them as well.

View a Device's Local Topology from the Device 360 View

You can launch a small topology window from the Device 360 view that displays the network topology around a device, up to 3 hops.

Step 1 Open the Device 360 View for the device in which you are interested.

- Click the "i" icon next to an IP address in almost any device table.
- From the network topology, click a device in an expanded group, then click **View**.

Step 2 Choose **N-Hop Topology** from the Actions drop-down menu (at the top right of the Device 360 view).

Step 3 Adjust the popup window to show the information you need.

- Click the edit icon
- Select a hop count (1-3) from the Hop drop-down list.
- Select a topology map layout from the Layout drop-down list.

Step 4 Save your changes, and use the pan and zoom tools to view the results.

View the Network's Hardware Inventory

Use this procedure to view basic hardware information for all devices in the network—the product name, physical location, serial number, manufacture date, and so forth.

Step 1 To view device-level information:

a. Choose **Inventory** > **Device Management** > **Network Inventory**.

b. Use the Quick Filters to locate specific devices. For example, to list the hardware information for all ASR devices, enter ***ASR*** in the Product Name field.

Step 2 To view element-level information, use one of these methods:

- Get the information from the Device Details page. See Get Complete Device Information: Device Details Page, on page 90.
- Get the information from the Chassis View. See Open the Chassis View, on page 92.
- Run a hardware report. See Device Reports, on page 291.

Get Complete Device Information: Device Details Page

For the most comprehensive information about a device, view the Device Details page. It provides in-depth inventory information and configuration options.

Figure 1: Chassis View Window

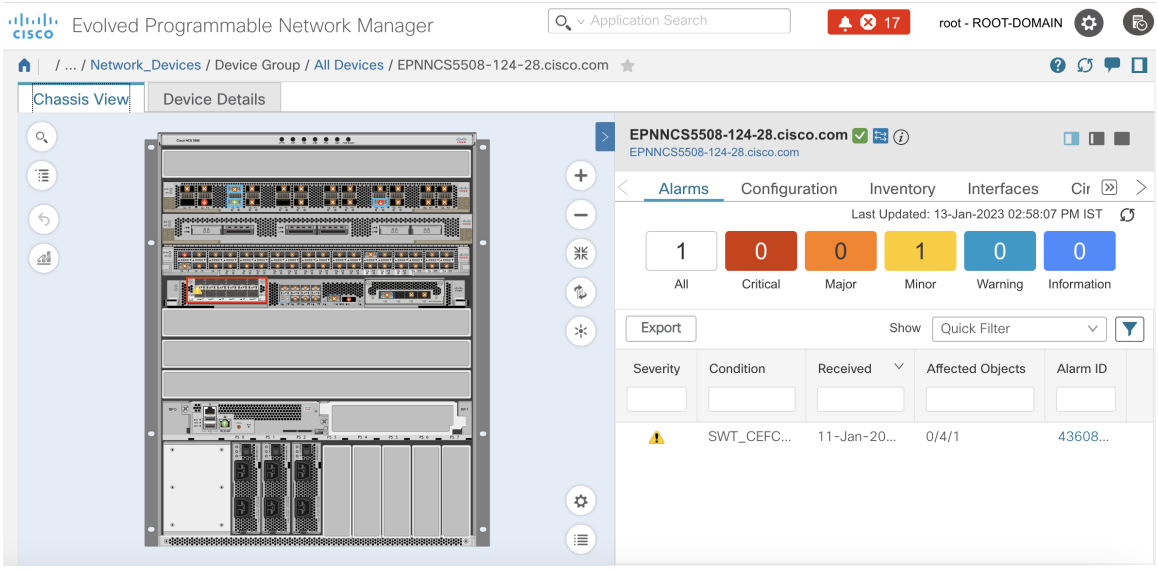
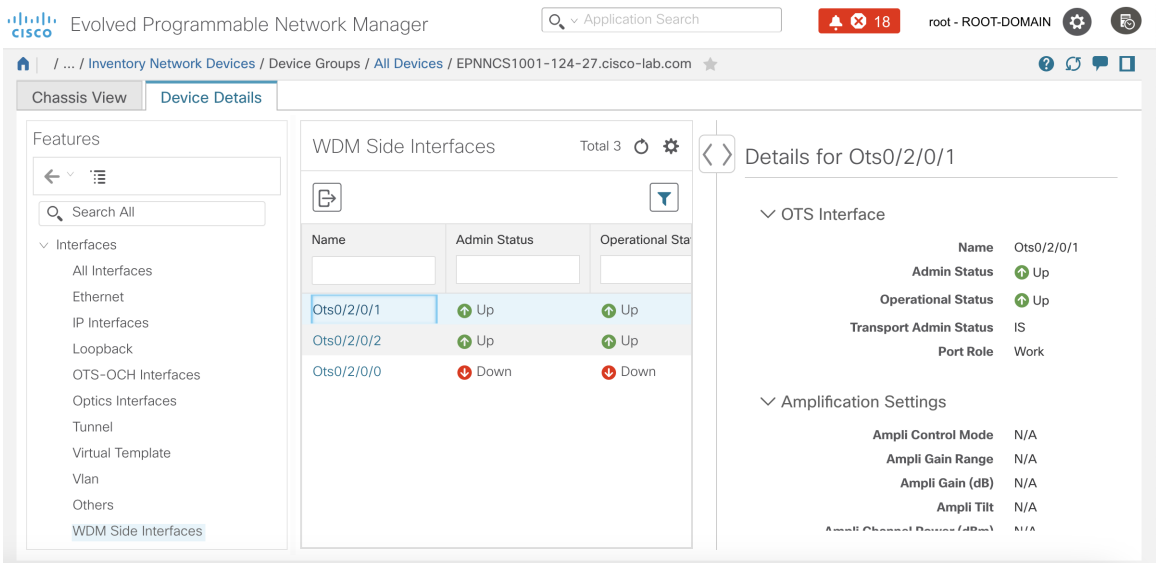


Figure 2: Device Details Window



To launch the Device Details Page:

- From a Device 360 view—Click the IP address hyperlink or choose **View** > **Details** > **Device Details** tab.

The tabs that are displayed here depend on your selection in the Chassis View. They are described in the following table:

Tab Name	Description
Chassis View	Provides inventory, service, and alarm information that is contextualized to the element you select. Also serves as launch point for configuration, Image management, and Configuration Archive features. For information on using the Chassis View features, see Overview of the Chassis View Window, on page 94.
Device Details	Provides system information (environment, modules ports, interfaces, and other settings). Provides logical inventory information and configuration options for these elements.
Alarms	Get information about the alarms that have been raised on a device, a card, or a port. See View an Alarm's Details, on page 258.
Configuration	Configure a device, card, or port. Elements are grouped by their physical location. (To configure elements that are grouped according to their logical function, click the **Device Details** tab.) See Ways to Configure Devices Using Cisco Evolved Programmable Network Manager, on page 313.
Inventory	View detailed hardware information such as serial numbers and manufacture dates for a device or card.

Tab Name	Description
Interfaces	View the status of interfaces configured on a device, card, or port. From here, you can also open the **Interface 360** view for a particular interface. For links to topics that describe other ways to view interface information in Cisco EPN Manager, see View Device Interfaces, on page 102.
Circuits	View the circuits a device, card, or port participates in. For links to topics that describe other ways to view circuit information in Cisco EPN Manager, see View Circuits/VCs, on page 109.
Image	Manage the software image that is running on the device. See View the Images That Are Saved in the Image Repository, on page 132. **Note** This tab is only available when a top-level chassis is selected.
Configuration Archive	Manage the device configuration file that is running on the device. See View All Archived Files. **Note** This tab is only available when a top-level chassis is selected.

To get an overview of a device, you can navigate to **Device Details** > **System** > **Summary**. Here you can view information such as device details, inventory details, port summary, NTP, SRLG, clock settings, and so on.

View and Manage Devices Using the Chassis View

The Chassis View provides an interactive model of a device chassis and its hardware elements. From the Chassis View you can:

- View the contents of a chassis.
- Check the state of chassis elements and locate problems.
- View alarmed elements and launch views that provide alarm details.
- Configure interfaces (using the launch point that opens the Device Details page).

The elements that are displayed in the Chassis View depend on the device type and the elements that are configured on the device.

Note Chassis View is not supported for Cisco Catalyst 8300 series and Cisco Catalyst 9300 series devices.

Open the Chassis View

The following table describes the various ways you can open the Chassis View. If a device does not provide these launch points, it means the device does not support the Chassis View. For a list of devices that support the Chassis View, see https://www.cisco.com/c/en/us/support/cloud-systems-management/evolved-programmable-network-epn-manager/products-device-support-tables-list.html.

To open a Chassis View from:	Do the following:	The Chassis View is displayed in:
Network Devices table	Click  next to the device IP address.	A pop-up window
	Click a device name hyperlink.	A full-page view
Device 360 view	Choose **View** > **Chassis View** from the top right of the **Device 360** view.	A pop-up window
	Choose **View** > **Details** from the top right of the **Device 360** view.	A full-page view
Device Details page	Click the **Chassis View** tab.	A full-page view

To open a full-page Chassis View from a Chassis View pop-up window, click the **Launch Configuration** link in the top right corner of the window.

Permissions Required to View and Configure Devices Using the Chassis View

The following table describes the Chassis View permissions that are granted to members of the Cisco Evolved Programmable Network Manager user groups. These permissions cannot be edited. For more information on user groups, see Control the Tasks Web Interface Users Can Perform, on page 792

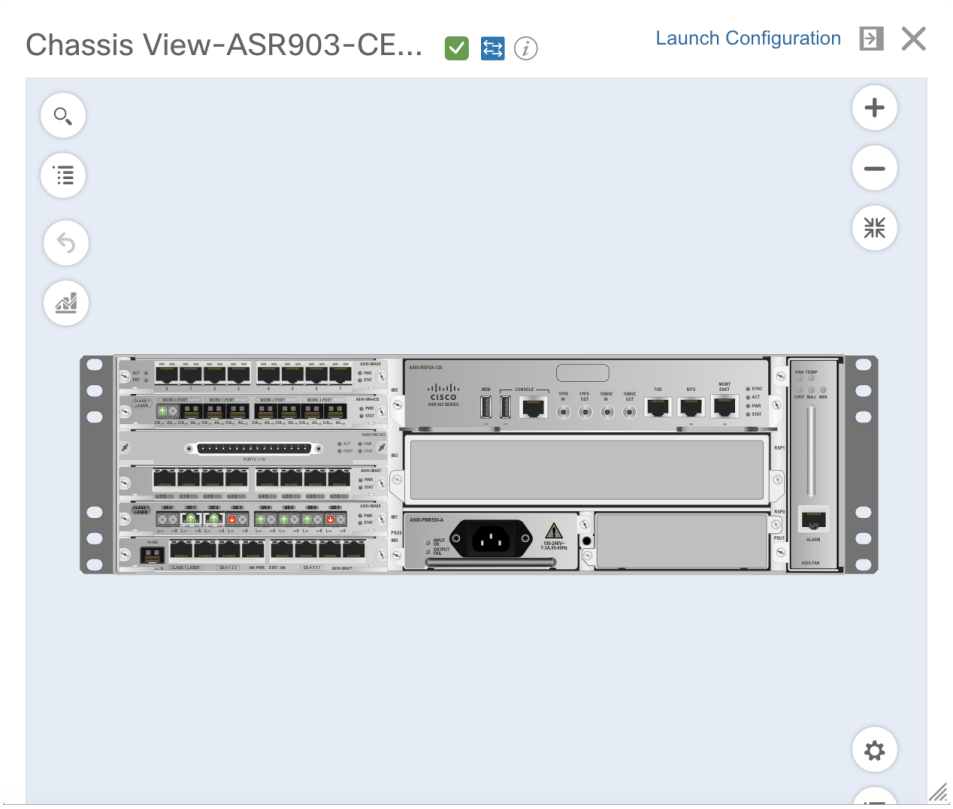
- Full access (read and write)—Users in this group can view and configure devices using the Chassis View.
- Read-only access—Users in this group can use the Chassis View to view devices but not to configure them.
- Write-only access—Users in this group can use the Chassis View to configure devices but not view them (only applies to the NBI Write group).
- No access—Users in this group cannot access or use the Chassis View.

Group Type		Read	Write
Web UI	Root	X	X
	Super Users	X	X
	Admin	—	—
	Config Managers	X	X
	System Monitoring	X	—
	User-Defined 1–4	X	—
	Monitor Lite	X	—

Group Type		Read	Write
NBI	NBI Read	X	—
	NBI Write	—	X
	North Bound API	X	X

Overview of the Chassis View Window

The following illustration shows the Chassis View for a Cisco ASR 903 router.



The Chassis View updates, displaying only the line card module that the port resides on and zooming in on it. The port pulsates in the Chassis View to help the user locate it. The badges that are displayed on the ports in this module indicate the primary status of those ports (see Port or Interface States, on page 97). Some elements may be surrounded by colored lines to indicate their state (out of service, preprovisioned, and so forth). To open a key that explains the meaning of the badges and these other indicators, click at the bottom right of the Chassis View.

If a device has multiple chassis or shelves, each chassis or shelf is displayed in the same Chassis View (for an example, see View Mixed Chassis, Multi-Chassis, and Multi-Shelf Devices in the Chassis View, on page 98). If a card image cannot be retrieved, the Chassis View displays a question mark alongside the card name.

You can customize the GUI display setting that controls the number of racks to be displayed in the chassis view. To do this:

1. Click at the top right of the Cisco EPN Manager window, then choose **My Preferences**.
2. Under **Chassis View Configuration**, in the **Chassis racks to display** drop-down list, choose a value. The specified number determines the number of racks to be displayed in the Chassis view. The default value is 2.

To improve loading time, the rack information is not displayed by default. You must click the download button (displayed on the rack) to display the relevant rack information.

Note

- The colors that are rendered in the Chassis View may not match your physical device because the Chassis View displays a generic image that is packaged with Cisco EPN Manager.
- If you have opened the Chassis View for a Cisco NCS 6000 device that houses a Secure Domain Router (SDR), the device type and the SDR's name are displayed at the top of the Chassis View. Keep in mind that there may be cases where the SDR label for a device that belongs to a cluster or a user-defined group is not displayed (since auto-clustering is applied to devices based on their proximity).

The following table describes the Chassis View components and their function:

Chassis View Component	Description
	Opens a field you can use to search for a particular rack, shelf, module, or interface on a device.
	Opens the **Chassis Explorer**.
	Indicates the device's reachability state (see Device Reachability and Admin States, on page 66). This example indicates the device is reachable.
	Indicates the device's administrative status (see Device Reachability and Admin States, on page 66). This example indicates that the device is managed.
	Opens the device's **Device 360** view. See Get Basic Device Information: Device 360 View.
Launch Configuration link	Opens the device's Device Details page. The tabs that are displayed on this page vary, depending on whether a device, module, or port is currently selected in the Chassis View. See Get Complete Device Information: Device Details Page.
	Adds a shortcut to the device's Chassis View in the **Dock** window. See Customize the Dock Window.
	Closes the **Chassis View**.
	Zooms in on an image.
	Zooms out from an image.

Chassis View Component	Description
	Resizes an image so it can be viewed in its entirety within the **Chassis View**.
	Toggles between the front and rear Chassis View for a device that supports this feature. A callout that appears when you place your cursor over this icon indicates which view you are opening. This feature is supported for the following Cisco devices: • Cisco ASR 901S routers • Cisco NCS 1001, 1002, 5001, 5002, and 5008 devices
	Rotates the image of the module that is currently displayed. This icon is not available when an entire device is displayed.
	Click to access the **Enable Alarm Blinking** check box. When checked, any alarm badges that are displayed for a module or port will blink in order to draw attention to them and make them easier to locate.
	Opens a key that explains the significance of badges and colored lines that are displayed in the **Chassis View**.
	Opens the performance graphs for the device.
	Takes you a level back in the view.

View Network Element State Information in the Chassis View

Badges, lines, and colors provide information about the operational state, elements and components in a device. Click the **Legends** icon at the bottom right of the Chassis View to display a key that lists what the badges, lines and colors mean.

See these topics for more information:

- Equipment Operational States (Chassis View), on page 96
- Port or Interface States, on page 97

Note Port state information is not shown for the CFP ports on an A9K-400G-DWDM-TR line card as these ports are not yet supported.

Equipment Operational States (Chassis View)

The equipment operational states represent the running state of the network element.

Equipment Operational State	Icon	Description

In Service	(none)	Equipment is operating properly.
Pre-provisioned		(Cisco NCS 2000 and Cisco ONS devices only) Equipment has been configured but is not physical present in the chassis.
Failed/Disabled/Down/Out of Service/Out of Service Maintenance		Equipment is not operating properly.
Unknown		Equipment operational state is unknown. No response (or insufficient response) from the device.

Port or Interface States

Port or Interface Primary States—Conveys the most important state information for a port or interface by combining the admin and operational states. The Multilayer Trace displays either a port's primary state or alarm status. For the Chassis View, if an element does not support the changing of color to indicate a state change, you can still get the state change information from the alarm that is generated.

Note If there is an alarm associated with a port/interface, alarm icon will show up, port icon will not show. The alarm is shown only in case the port is not in test or admin down state.

Port or Interface Primary State	Icon	Admin Status	Operational State
Unknown		Unknown	Unknown
Down		Up	Down
Testing		Test	—
Admin Down		Admin Down	—
Up		Up	Up
Auto Up		Up	Auto Up

Port or Interface Admin Status—Represents the configured state of the port or interface (for example, if an administrator has manually shut down a port).

Port or Interface Admin Status	Icon	Description
Unknown		Port or interface admin status is unknown. There is no response (or insufficient response) from the device.
Admin Down		Port or interface was manually shut down by the administrator.

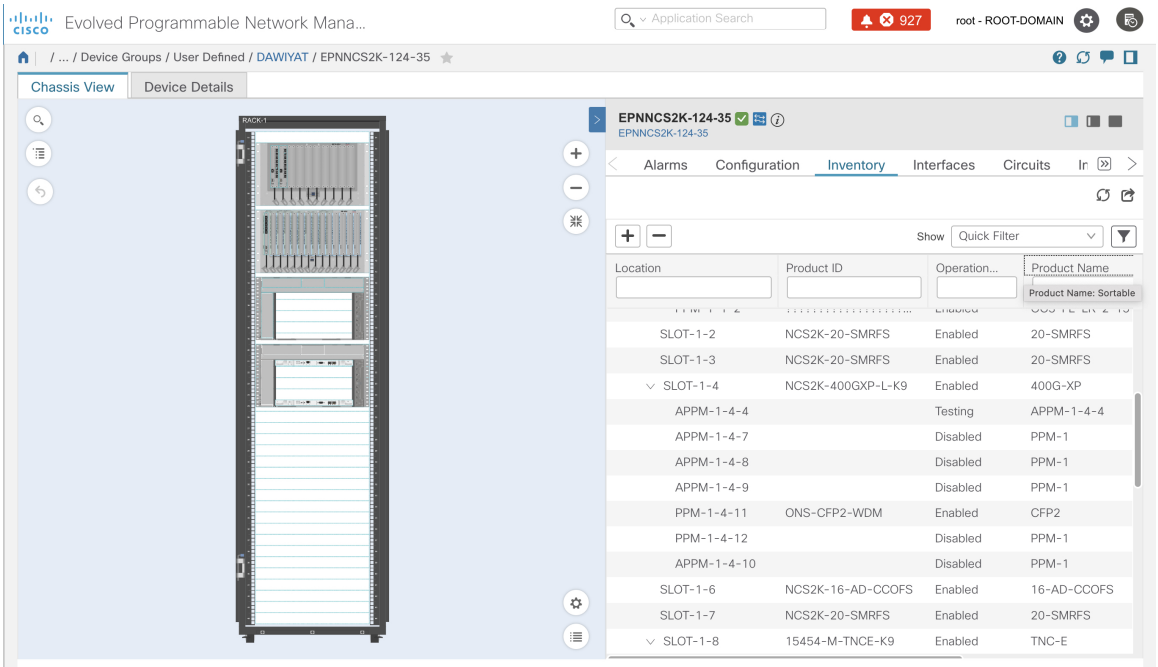
Up		Port or interface is enabled by the administrator.
Testing		Port or interface is being tested by the administrator.

Port or Interface Operational State—Conveys the port or interface's running state and whether it is working properly.

Port or Interface Operational State	Icon	Description
Unknown		Port or interface operational state is unknown. There is no response (or insufficient response) from the device.
Down		Port or interface is not working properly.
Up		Port or interface is receiving and transmitting data.
Auto Up		Port or interface is receiving and transmitting data (only certain devices support this state; other devices use "Up").

View Mixed Chassis, Multi-Chassis, and Multi-Shelf Devices in the Chassis View

The following example shows a mixed Chassis View. Shelf numbers are not consecutive because of the different types of chassis.



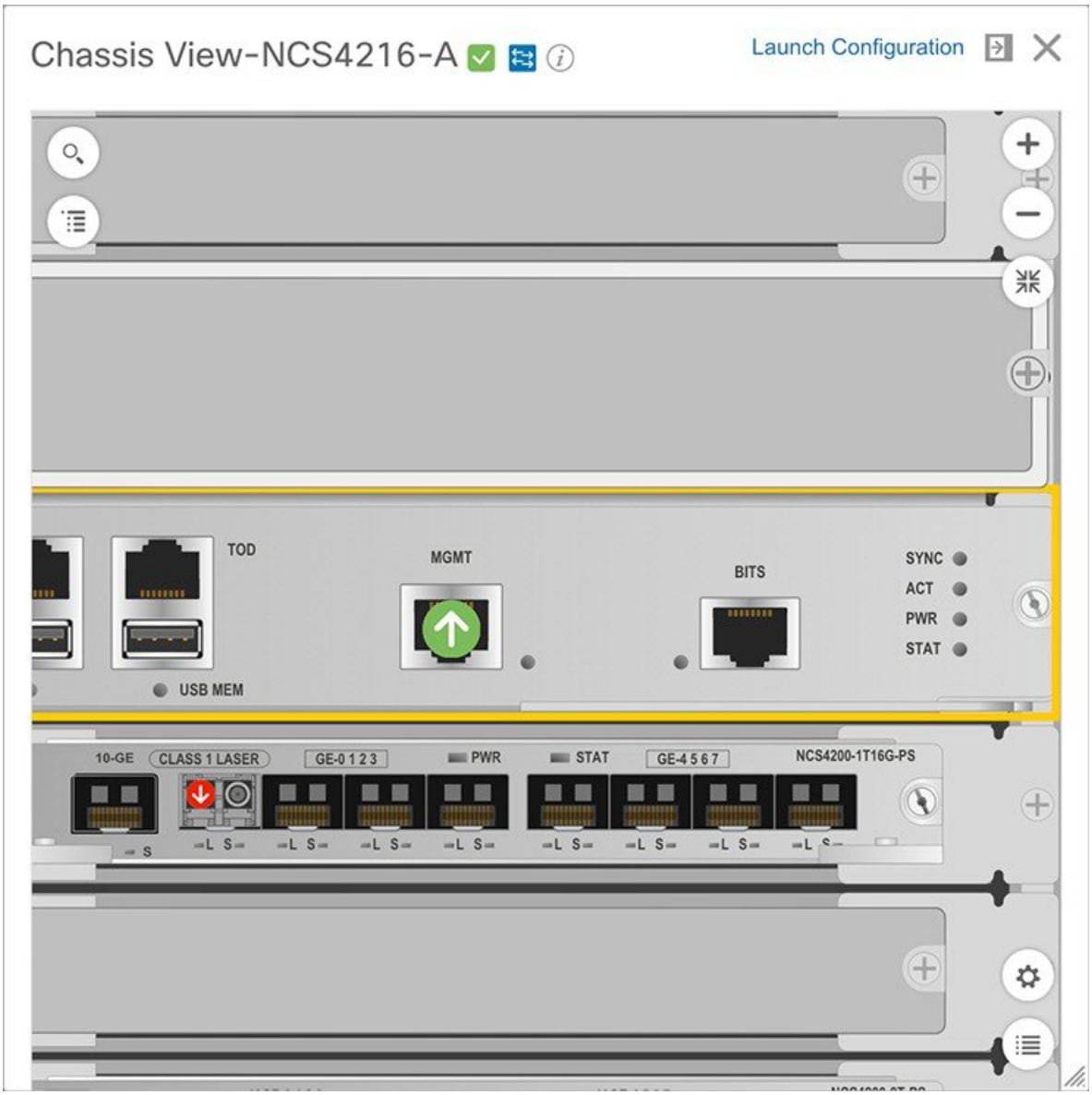
For mixed-chassis, multi-chassis, and multi-shelf devices, Cisco EPN Manager aggregates alarms to a chassis or shelf as explained in View Alarms in the Chassis View, on page 99.

For multi-chassis devices in a cluster, the Device 360 view's **Chassis** tab identifies which chassis is the primary and which is the backup.

Note Chassis View opened for a multi-shelf device will display only the first four racks, and requires the user to click the download button (displayed on the rack number 5 and above) to display the relevant rack information.

View Alarms in the Chassis View

An alarm badge in the Chassis View represents one or more alarms that have been localized to a piece of equipment. For an element with multiple alarms, the badge icon will convey the most severe alarm.



To customize the Chassis View so that alarm icons blink (to bring your attention them), click  from the bottom right of the view, then check the **Enable Alarm Blinking** check box.

Note If there is an alarm associated with a port/interface, alarm icon will show up, port icon will not show. The alarm is shown only in case the port is not in test or admin down state.

To view the alarms specific to a device, do the following:

Step 1 With a device's Chassis View open, click the **Launch Configuration** link.

The Device Details page opens.

Step 2 If not already selected, click the **Alarms** tab.

All of the alarms that have been raised for the device are listed here.

Step 3 To view the alarms for a specific device component (such as a line card or port), do one of the following:

- Double-click the component in the Chassis View.
- Click  to open the **Chassis Explorer**, then click its entry.

View Routes of a Circuit in the Chassis View

You can view the end-to-end physical route of a circuit using the Chassis View of a device participating in the circuit. You can also choose to view the power levels and span loss in the circuit.

Note This feature is available only for the OCH WSON Optical circuit type.

Step 1 From the left sidebar, choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 From the Network Devices table, click the required device's name hyperlink to open the full-page view of the Chassis View.

Step 3 Expand the Chassis View Explorer, and then select the shelf.

Step 4 In the right pane, click the **Circuits** sub-tab, and then select the circuit for which you want to view the physical routes.

The Chassis View displays the physical routes of the circuit. The internal connections between the ports of the same card are displayed as dotted lines.

Step 5 In the left pane, next to the Chassis View, click the eye icon to show or hide the physical routes, power levels, and span loss.

View Device Ports

You can get in-depth information about a device's physical ports from the Device Details page. You can also get basic port information from various 360 views.

To view a device chassis with its modules and ports, use the Chassis View. See Open the Chassis View, on page 92.

To view this port information:	Do the following:

All Physical ports on a device (including port alias and residing module)	1. Open the Device Details page. • Choose **View** > **Details** from the top right of the Device 360 view. • Click the device name hyperlink in a device table. 2. Under the **Device Details** tab, choose **System** > **Physical Ports**.
An interface's ports	Check the **Interface** tab on a 360 view.
Ports connected to a module	Check the **Modules** tab on a Device 360 view.
Ports connected to a neighbor	Check the **Neighbors** tab on a Device 360 view.

For a matrix of ports states and icons, see Port or Interface States, on page 97.

View Device Interfaces

Cisco EPN Manager provides the following ways to view device interfaces:

Ways to View Interfaces	For more information, see:
View details about a specific interface	Get a Quick Look at a Device Interface: Interface 360 View, on page 103
View a specific device's interfaces	• View a Specific Device's Interfaces: Device 360 View, on page 102 • Get Comprehensive Information About a Device's Interfaces Using the Device Details Page, on page 106 • View Interfaces in the Chassis View, on page 107

View a Specific Device's Interfaces: Device 360 View

Use the Device 360 view to quickly check the status of a device's interfaces.

Step 1 Open the Device 360 view:

- Click the "i" icon next to an IP address in almost any device table
- From the network topology, click a device in an expanded group, then click **View**

Step 2 Click the **Interfaces** tab.

Get a Quick Look at a Device Interface: Interface 360 View

The Interface 360 view shows summary information for a specific interface including general interface details, interface status, alarms on the interface, circuits/VCs traversing the interface, and performance information. From the Interface 360 view's **Actions** menu, you can perform basic tasks such as enabling and disabling the interface, and so on. The **Show in Topology** option launches the topology map so that you can view the interface in the context of the map.

You can launch the Interface 360 view wherever you see an "i" icon next to an interface name—for example, in an alarms table, a links table or in a device 360 view.

The Interface 360 view provides general interface information at the top of the view, and more detailed interface information in tabs in the lower part of the view. The information the Interface 360 view displays depends on the interface configuration.

The tabs displayed vary depending on the type of interface for which you launched this view. For example, for optical interfaces you might see the Optical Physical tab or the ODU tab, depending on the type of optical interface.

Note Interface 360 has a limited IPv6 support.

Using the menus in the pop-up window, you can also perform these tasks:

- Auto-Refresh—For real-time updates of status and troubleshooting, enable an on-demand refresh by clicking on the Refresh icon. Alternatively, you can also set the autorefresh interval to 30 seconds, 1 minute, 2 minutes or 5 minutes from the drop-down list. Auto-Refresh is OFF by default.

Note The Auto-Refresh setting is applicable only for the currently open 360 view popup window. If the view is closed and reopened or another view is opened, by default Auto-Refresh is Off.

- Open a chassis view that highlights the port or line card the interface is associated with (**View** menu). This feature comes in handy when you need to describe to an onsite technician where to find the source of an issue.
- Select the interface for a side-by-side comparison with another interface based on information such as raised alarms and the status of associated circuits and VCs (**Actions** menu)—see Compare Interface Information and Status, on page 105.
- View performance information in the relevant performance dashboard for the specific interface type by selecting **View > Performance**.
- Enable and disable the interface from the **Actions** menu.
- Enable and disable the lockout of an MPLS interface from the **Actions** menu. You would lock out an MPLS interface before doing maintenance work on the MPLS TE Tunnel link that the interface belongs to. Close and reopen the Interface 360 View to see the updated details.

Note MPLS Lockout is not applicable on tunnel interfaces.

The MPLS Lockout is only applicable on interfaces that have a valid discovered MPLS link in EPNM.

- View the device on which the interface is located in a topology map (**Actions** menu).
- Enable testing for the interface from the **Actions** menu.
- Enable with AINS from the **Actions** menu.
- Copy and activate a port configuration from one port to another using **Actions** > **Migrate Port**. This operation is supported only on XR devices. You can select only the empty destination ports (no configuration exists on the ports) while performing this operation. Use the **`show running-config interface`** `<dest port>` command to confirm that the destination port is empty. After the operation is successful, the source port will be shut down.
  - Both source and destination ports cannot be same.
  - Source and destination ports can be from different cards, however, they must be of the same type (for example, if the Source Port is Gigabit Ethernet, then the Destination Port should be of Gigabit Ethernet).
  - The migrate port operation is applicable only on Ethernet physical ports.

  Recommendation is to move the device to maintenance mode before performing the migrate port operation. This operation is based on the functionality provided by XR platform: the device must support the **`replace`** CLI command.

Warning Migrating of port configuration that is configured with service endpoints create a gap between the intent and the discovered service. It is not possible to address this issue with service reconciliation, as changes in the service endpoints cannot be reconciled.

- To clear the alarms of the migrated ports, you can use the following API:

  ```
  https://<Server
  IP>/webacs/alarm-rest/ClearAlarmsByPort?portName=<Port_Name>&deviceIp=<Device IP>
  ```

  Where,
  - **`<Server IP>`** is the IP address of the server.
  - **`<Port_Name>`** is the name of the port where the device is configured.
  - **`<Device IP>`** is the IP address of the device.
- Set a baseline for performance data for optical interfaces (except for optical physical interfaces) for troubleshooting purposes. See Set a Baseline for Optical Performance Data, on page 107 for more information.
- Use the **UPSR/SNCP Protection** option under the **Actions** menu to configure the switching pattern from the working interface to the protection interface on the device. This option is available in GUI only for

devices whose Working and Protection Interfaces are configured. Cisco EPN Manager regularly syncs the inventory database with the device interface, based on user settings. The options to switch the interfaces are progressive:

- Lockout - Prevents a working interface from switching to a protect interface.
- Force Protect - Switches to a protect interface.
- Force Working - Switches to a working interface.
- Manual Protect - Manually switches to a protect interface.
- Manual Working - Manually switches to a working interface.
- Clear - Clears previously set external command.

Information Provided in Interface 360 View	Description
General information	The interface name, status, description, type, device name; IP address, MAC address, and so forth.
Performance data	Launch point to the relevant performance dashboard from **View** > **Performance**.
Alarms	Current alarms for the interface, including their severity, status, and the time they were generated. Also provides a launch point to the Alarm Browser.
Interfaces	Name, interface type, and operational and admin status for each associated interface. Also provides a launch point for the Interface 360 view.
Circuits/VCs	(For interfaces that participate in circuits) Circuit/VC name, type, customer, status, and creation date. Also provides a launch point for the Circuit/VC 360 view.
EFPs	All EFPs associated with the interface (if relevant). Also provides their operational status, admin status, and EFP type.
Detailed information relevant to a specific interface type.	Additional interface information and performance data in tabs relevant to the type of interface, for example, Optical Physical, ODU, FEC, and so on. **Note** From release 7.0 onwards, performance metrics **Pre FEC BER** and **Post FEC BER** are removed from the **Coherent DSP Controllers** page and added under the **Interface/FEC** tab.
Optical Physical	Real-time performance monitoring data for the interface. This data is collected every 10 seconds, and the results of the last 12 pollings are displayed here. For a listing of the counters that can be displayed, see Performance Counters for Optical Monitoring Policies.

Compare Interface Information and Status

From the **Comparison View** page, you can perform a side-by-side comparison of multiple interfaces, viewing information such as IP and MAC address, raised alarms, and associated circuits and VCs. To compare interfaces, do the following:

Step 1 For each interface you want to compare:

a) Open its **Interface 360** view, as described in Get a Quick Look at a Device Interface: Interface 360 View, on page 103.

b) Choose **Actions** > **Add to Compare**.

The interface you selected is displayed at the bottom of the page. You can select a maximum of 4 interfaces.

Step 2 Click **Compare**.

The **Comparison View** page opens.

Step 3 From the drop-down list at the top of the view, specify whether the view will show all available information or just the information that is unique to each interface.

Step 4 Click **Customize View**, check the check boxes for the categories you want the view to display, and then click **Save**.

By default, all the categories are selected.

Step 5 Scroll down the page to view the information provided for each category you selected.

Note the following:

- The **Comparison View** only displays information for two interfaces at a time. If you selected more than two, you will need to toggle to the interfaces that are not currently displayed.
- To reorder the interfaces you have selected, click **Rearrange**.
- Each interface's **View** and **Actions** menu is identical to the ones provided in its **Interface 360** view. If you select an option, the corresponding page opens.
- You can minimize and maximize the categories displayed, as needed.
- The **Comparison View** is also available for circuits and VCs, devices, and links. Whenever you select any of these elements from their respective 360 view for comparison, they are displayed in the corresponding tab. This allows you to switch between element types, as needed.
- When you are done comparing interfaces, click **Back** at the top of the page and then click **Clear All Items** at the bottom of the page. If tabs for other element types are still displayed, you will need to clear them as well.

Get Comprehensive Information About a Device's Interfaces Using the Device Details Page

Use the Device Details page to get extensive information about all of the interfaces that are configured on a device. For easier navigation, interfaces are grouped together by type.

Step 1 Open the Device Details page.

- Click the device name hyperlink which appears in many of the device tables
- Choose **View** > **Details** at the top right of the Device 360 view

Step 2 Under the Device Details tab, double-click **Interfaces** to display a list of all interfaces (of all types) that are configured on the device.

Step 3 To display all interfaces of the same type, click the type (such as **Ethernet Interfaces**).

Step 4 To get details about a specific interface, click the interface name hyperlink.

View Interfaces in the Chassis View

You can view the interfaces and their details using the Chassis View of a device participating in the circuit. You can find the interface details such as name, alarm, location, interface type, admin status, operational status, transport admin status, and serial number of the modules.

Step 1 From the left sidebar, choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 From the Network Devices table, click the required device name hyperlink to open a full-page view of the Chassis View.

Step 3 Expand the Chassis View Explorer, and then select the shelf.

Step 4 In the right pane, click the **Interfaces** subtab.

Set a Baseline for Optical Performance Data

Setting a baseline for optical interface performance data enables you to compare realtime network performance with a fixed set of performance statistics. In this way, you could compare normal baseline network performance with abnormal network behavior.

After you set a baseline, all new incoming performance statistics are recalculated based on the baseline values to show you the difference between the baseline values and the current realtime values (specifically, the current value minus the baseline value).

Optical interfaces that support this functionality will have a **Set Baseline** button in the relevant tab in the Interface 360 view.

To set a baseline for optical interface performance statistics:

Step 1 Open the Interface 360 view for the relevant interface.

Step 2 Open the tab specific to the interface type, for example, FEC, OTU, and so on.

Step 3 Click the **Set Baseline** button.

The rows in the table will be cleared. Each new row will have values that reflect the difference between the baseline values and the current realtime values.

Step 4 To go back to the realtime values (effectively removing the baseline), close the Interface 360 view and then reopen it.

View Device Modules

To view device module information, choose **Inventory > Device Management > Network Devices**, then launch a Device 360 or Device Details page, depending on how much information you want.

To get this information:	Use this navigation:
Basic module information: Status, type, ports	From the Device 360 view, click the **Modules** tab. To open the Device 360 view: • Click the "i" icon next to the IP address in almost any device table. • From the Network Topology, click a device (in an expanded view), then click **View**.
Module equipment type and power information	From the Device Details page, choose **System > Modules** under the Device Details tab. To open the Device Details page: • Click the device name hyperlink which appears in almost any device table. • Choose **View > Details** from the top right of the Device 360 view. **Note** Due to a limitation in the retrieval of module related information, this page lists SFP transceivers of Cisco CAT6500 devices as 'Unspecified' products.

View Environment Information (Power Supplies, Fans)

Environment-related information, such as details about power supplies and fans, is displayed in the **Device Details** page. To access this information:

Step 1 Follow either of the following steps:

- Click the device name hyperlink that appears in almost any device table and then click the **Device Details** tab.
- Choose **View > Details** from the top right of a **Device 360** view and then click the **Device Details** tab.

Step 2 From the **Features** pane on the left, choose **System** > **Power Options & Fans** or **System** > **Environment** (depends on the device type).

View Device Neighbors

Device neighbor information, such as the neighbor name, port number, index, and duplex setting, is displayed in a device's **Device 360** view.

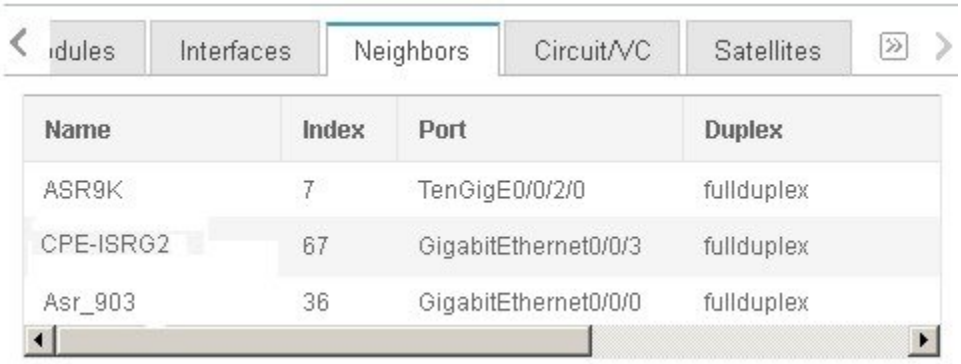
Step 1 Open the **Device 360** view:

- Click the *i* (**information**) icon next to the IP address in almost any device table.
- From the network topology, click a device in an expanded group and click **View**.

Step 2 Click the **Neighbors** tab.

Example

For example:



Get More Information About Links

Cisco EPN Manager provides a variety of ways that you can view links and get more details about them:

To view link information for:	See the procedures in:
A specific link	Get a Quick Look at a Specific Link: Link 360 View, on page 186
A specific link in a topology map	View a Specific Link in the Topology Map, on page 189
A group in a topology map	View a Device Group's Links in a Network Topology Map, on page 189
All of Cisco EPN Manager	View Link Tables , on page 190

View Circuits/VCs

Cisco Evolved Programmable Network Manager provides a variety of ways that you can view circuits/VCs:

To view circuit/VC information for:	See the procedures in:

A specific circuit/VC in a topology map, in a Circuit/VC 360 view, or in a Circuit/VC Details page	• Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 629 • Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window, on page 635
A device	View a Specific Device's Circuits/VCs, on page 637
A device group in a topology map or in an expanded table	View a Device Group's Circuits/VCs, on page 638
All of Cisco Evolved Programmable Network Manager	View All Circuits/VCs in Cisco EPN Manager, on page 639

View Satellites

Cisco Evolved Programmable Network Manager provides the following ways to view satellite information for host-satellite configurations:

Ways to View Satellites	For more information, see:
View all satellites in a location group using a topology map	View Cisco ASR 9000 Host-Satellite Topologies in the Topology Map, on page 272
View a specific device's satellites from a Device 360 view	• Identify the Satellites Connected to a Cisco ASR 9000 Host, on page 273 • Get Basic Device Information: Device 360 View, on page 84
View details about a specific satellite, including the hosts it is connected to, using the Satellite 360 view	Identify the Hosts Connected to a Satellite, on page 274

Create User Defined Fields for Custom Values

If you want to assign custom attributes to devices or circuits/VCs, you can create your own fields to be shown in the tables and you can define custom values in those fields. For example, you might want to label certain devices with a customer name. After you have created user defined fields and assigned values, you can search by these values in the tables.

To create user defined fields:

Step 1 Choose **Administration** > **Settings** > **System Settings** > **General** > **User Defined Fields**.

Step 2 Click the + icon. Select type of user defined field (UDF) from the drop-down list and enter a label and description.

Step 3 Assign values in your newly created user defined field for specific devices/circuits/VCs as follows:

a) Go to the device table or to the table of circuits/VCs.

b) Display your user defined field as a column in the table by clicking the settings icon at the top right of the table, choosing **Columns**, and then selecting your user defined field.
c) Go to the required device or circuit/VC in the table, enter a value in your user defined column, and click **Save**.

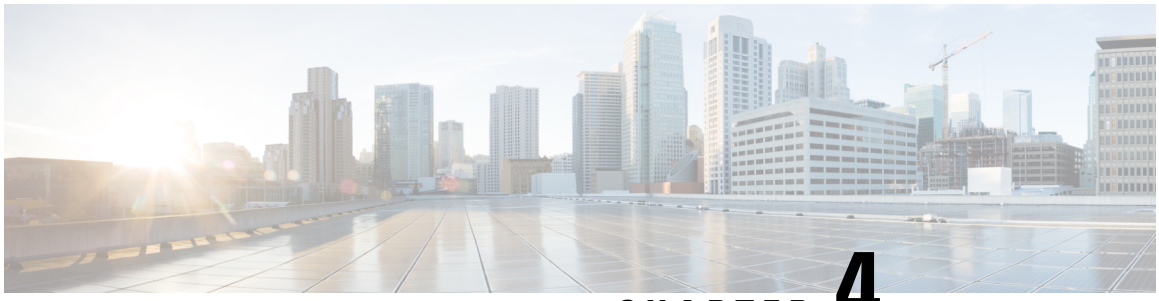
Delete User Defined Fields

To delete user defined fields:

Step 1 Choose **Administration** > **Settings** > **System Settings** > **General** > **User Defined Fields**.

Step 2 Select the user defined fields that you want to delete and click the Delete icon.

This deletes the selected user defined fields.



CHAPTER 4

Manage Device Configuration Files

Set Up Device Configuration File Management

Make Sure Devices Are Configured Correctly

Cisco Evolved Programmable Network Manager can transfer files to and from devices only if the SNMP read-write community strings configured on your devices match the strings that were specified when the devices were added to Cisco Evolved Programmable Network Manager. In addition, devices must be configured according to the settings in How Is Inventory Collected?, on page 52.

Note To improve security, Cisco Evolved Programmable Network Manager no longer uses some of the SSH CBC (Cipher Block Chaining) ciphers that older Cisco IOS-XE and IOS-XR versions use, as they have been deemed weak. For devices running Cisco IOS-XE, ensure that you upgrade to version 16.5.x or later. And for devices running Cisco IOS-XR, upgrade to version 6.1.2 or later. Otherwise, several Software Image Management operations will fail.

Although we do not recommend doing so (since it weakens security), you also have the option to add the CBC ciphers that Cisco Evolved Programmable Network Manager stopped using back to its SSHD service configuration file. To do so, first configure the CBC ciphers in the ciphers line of the file located in the **/etc/ssh/sshd_config** directory (as shown in the example below), then restart the sshd service using the **service sshd stop/start** command.

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,
arcfour256,arcfour128,aes128-cbc,3des-cbc,
cast128-cbc,aes192-cbc,aes256-cbc
```

Note Software Image Management is not supported in the NAT environment. This means that image management features such as image import, upgrade, distribution, and activation, will not function in the NAT environment.

Control How Archiving is Triggered

By default, Cisco EPN Manager saves device configuration files to the archive when:

- A new device is added to Cisco EPN Manager.
- When a device change notification is received.
- Archive collection is not carried out in case of full or granular sync.

Note If there is an event occurrence, archive data is collected after the period of configured hold off timer.

Users with Administrator privileges can change these settings.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Configuration Archive**.

Step 2 Adjust the archiving settings depending on the following criteria.

Check this check box:	To archive files:
Archive configuration while adding a device	When a new device is added (enabled by default)
Collect Configuration Archive whenever configuration is changed	When a configuration change notification is sent (enabled by default); see Set Up Event-Triggered Archiving, on page 115

Step 3 To schedule regular archiving for groups of devices (or single devices):

a) Choose **Inventory** > **Device Management** > **Configuration Archive**.
b) Under the **Devices** tab, select the devices or device groups that you want to archive regularly.
c) Click **Schedule Archive Collection** and complete the schedule settings in the **Recurrence** area. If the operation is performed on many devices, schedule the archiving for a time that is least likely to impact production.
d) Click the **Backup to Repository** button to transfer device configuration periodically to external repository. You can configure or create the repository using CLI commands and the supported repositories are FTP, SSH FTP (SFTP), and Network File System (NFS). You can also select to encrypt the exported files using GnuPG. You have to provide an encryption password if you choose to encrypt using GnuPG.

Set Up Event-Triggered Archiving

By default, Cisco EPN Manager backs up a device's configuration files whenever it receives a change notification event. This works only if devices are configured correctly, see How Is Inventory Collected?, on page 52. For example, for devices running Cisco IOS XR and Cisco IOS XE, the following setting must be configured:

```
logging server-IP
```

When Cisco EPN Manager receives a configuration change event, it waits 10 minutes (by default) before archiving in case more configuration change events are received. This prevents multiple collection processes from running at the same time. To check or change this setting, choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Configuration Archive** and adjust the **Hold Off Timer (min)**.

Note The **Hold Off Timer** may be set to a shorter period for certain events, called expedited events. For more information, see Change the Behavior of Expedited Events, on page 856.

To turn off event-triggered archiving, choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Configuration Archive** and uncheck the **Collect Configuration Archive whenever configuration is changed** check box.

Specify Items to be Excluded When Configuration Files Are Checked for Changes

Some lines in device configuration files should be excluded when Cisco Evolved Programmable Network Manager compares different versions to identify changes. Cisco Evolved Programmable Network Manager excludes some lines by default, such as clock settings for routers and switches. If you have Administrator privileges, you can check which lines are excluded, and add more lines to be excluded.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Configuration Archive**.
Step 2 Click the **Advanced** tab.
Step 3 In the **Product Family** list, choose the devices or groups to which you want to apply the command exclusions.
Step 4 In the **Command Exclude List**, enter a comma-separated list of configuration commands you want to exclude for that selection. These are the parameters Cisco Evolved Programmable Network Manager will ignore when checking devices for configuration changes.

Step 5 Click **Save**.

Control the Timeouts for Configuration Archive Operations

The Configuration Archive task uses the Device CLI Timeout value for each fetch activity. A single Configuration Archive task entails 1 to 5 files. Consequently, the overall job timeout value is determined using the following logic:**Overall job timeout = Number of files*Device CLI Timeout**

To configure a CLI timeout value, choose **Inventory** > **Device Management** > **Network Devices**, click the edit device icon, select the **Telnet/SSH** option, and then enter a value in the **Timeout** field.

Note You must increase the Device CLI timeout value if the Configuration Archive task fails due to CLI timeout.

Control How Often Alarms are Triggered

By default, Cisco Evolved Programmable Network Manager saves device configuration files to the archive based on the configured settings. However, when these jobs fail, you can choose to generate an alarm notification.

When a Configuration Archive job fails, Cisco Evolved Programmable Network Manager waits for 7 days or for more than 5 (by default) configuration files before triggering an alarm. The alarm has information about the cause for the trigger of the alarm and other related details associated with the configuration archives. To change the default settings for how often the alarms are generated, choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Configuration Archive**, and adjust the **Alarm Threshold** parameter for maximum number of configuration files (exceeding which an alarm is generated) and the number of days to wait before the alarm is triggered.

Control When Device Configuration Files are Purged from the Database

Device configuration files cannot be automatically deleted from the database (you can manually delete the files); they can be periodically purged by Cisco Evolved Programmable Network Manager based on your settings. Users with Administrator privileges can adjust when configuration files are purged as follows. If you do not want any configuration files purged, follow this procedure but leave both fields blank.

Note For a description of how to manually delete a configuration file, see Delete Archived Device Configuration Files.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Configuration Archive**.

Step 2 Adjust the archiving settings depending on the following criteria.

Use this field:	To purge files when:
Max. configuration archive	The number of a device's configuration files exceeds this setting (5 by default).

Use this field:	To purge files when:
Max. days retained	A configuration file's age exceeds this setting (7 days by default).

How Do I Determine When Files Are Last Archived?

Step 1 To find the most recent date when the device running configuration files are backed up to the archive, navigate to **Inventory > Device Management > Configuration Archive**, and click the **Devices** tab. The **Latest Archive** column lists the archiving time stamp for each device with the most recent archive listed first.

The **Created By** column in the **Archives** tab displays the archive trigger (for example, a syslog).

Step 2 To view the most recently archived running configuration file contents of a device, click the time stamp hyperlink. The **Running Configuration** window displays the contents of the file.

To view the changes that are made among archives for a device, see Compare or Delete Device Configuration Files, on page 122.

Back Up Device Configuration Files to the Archive

What Is Backed Up to the Database?

The configuration archive maintains copies of device configuration files, storing them in the database. Most configuration files are stored in readable format as received from the device and can be compared with earlier versions. Device configurations can be restored to earlier states using the files saved in the archive.

If the running configurations and startup configurations on a device are similar, then the Cisco EPN Manager copies only the running configuration to the database. This is why in some cases, when you view the image repository, you will only see an archive for the running configuration.

If a configuration file has not changed since its last backup, then the Cisco EPN Manager does not archive the file. Cisco EPN Manager reports that the job was successful and the job result displays **Already Exists**.

Cisco EPN Manager collects and archives the following device configuration files.

Device/Device OS	What is Backed Up
Cisco IOS and Cisco IOS-XE	Latest startup, running, and VLAN configuration.

Device/Device OS	What is Backed Up
Cisco IOS-XR	• Latest running configuration, includes active packages. Devices must be managed with a system user because copy command is not available in command-line interface (CLI) for non-system users. • Database configuration (binary file). **Note** For Cisco NCS 1010 devices, only latest running configuration is backed up. **Note** For Cisco NCS 4000 devices, the database is backed up as a .tgz file to a file system on your local machine.
Cisco NCS devices	Database configuration (binary file). **Note** For Cisco NCS 2000 devices, the database is backed up as a binary file. Because it is not a text file, you cannot compare versions, but you can identify them by their file time stamps in the configuration archive.

Back Up (Archive) Configuration Files

When a configuration file is backed up, Cisco Evolved Programmable Network Manager fetches a copy of the configuration file from the device and copies (backs it up) to the configuration archive (database). Before saving a copy to the archive, Cisco Evolved Programmable Network Manager compares the fetched file with the last version in the archive (of the same type—running with running, startup with startup). Cisco Evolved Programmable Network Manager archives the file only if the two files are different. If the number of archived versions exceeds the maximum (5, by default), the oldest archive is purged.

For devices that support both running and startup configurations, Cisco Evolved Programmable Network Manager identifies *out-of-sync* (unsynchronized) devices during the backup process by comparing the latest version of the startup configuration with the latest version of the running configuration file. For more information on out-of-sync devices, see Synchronize Running and Startup Device Configurations, on page 121.

The following table describes the supported backup methods and how they are triggered. To check or adjust the default settings, see Control How Archiving is Triggered, on page 114.

When you archive a Cisco NCS 2000 database, if you receive an error message saying the database or flash is busy, it is likely caused by one of the following:

- You are performing the archive operation in parallel with other Configuration Archive or Image Management operations. You should retry the operation after a short period of time.
- Multiple users are performing the same operation at the same time. You should retry the operation after a short period of time.
- The device has a software download alarm that has not been cleared. You should clear the alarm.

Table 10: Backup Method

Backup Method	Description	Notes
On-demand manual backup	Choose **Inventory > Device Management > Configuration Archive**, choose devices, and click **Schedule Archive Collection** (run the job immediately or at a later time).	N/A
Regular scheduled backups	Choose **Inventory > Device Management > Configuration Archive**, choose devices, and click **Schedule Archive Collection** . In the scheduler, specify a **Recurrence**.	N/A
New device backups	Cisco Evolved Programmable Network Manager automatically performs backup for new devices.	Enabled by default
Event-triggered backups (device change notifications)	Cisco Evolved Programmable Network Manager automatically performs backup when it receives a syslog from a managed device.	Enabled by default

View the Device Configuration Files That Are Saved in the Archive

- View All Archived Files, on page 119
- View Archived Files for a Specific Device, on page 120

View All Archived Files

To view the configuration files that are saved in the database, choose **Inventory > Device Management > Configuration Archive**. Click the Archives or Devices tabs depending on where you want to start:

- **Archives** tab—A list of configuration files that have been archived, with the most recent archives listed first. The Out of Band column indicates whether the change was made by an application other than Cisco Evolved Programmable Network Manager. Use the Groups list on the left to view archives by device types and families. From here you can:
  - Roll Back a Device's Configuration To an Archived Version, on page 124
  - Overwrite a Startup Configuration with a Running Configuration, on page 124
  - Label Important Configuration Files With Tags, on page 121
- **Devices** tab—A flat list of devices with their archived configurations. From here you can:
  - Schedule backups to the archive (see Back Up Device Configuration Files to the Archive, on page 117).
  - View the archived file for a specific device by clicking the device name hyperlink (see View Archived Files for a Specific Device, on page 120).

By default, Cisco Evolved Programmable Network Manager saves up to 5 versions of a file, and deletes any files that are older than 7 days; device configuration files cannot be manually deleted from the database. (To check the current purging settings, see Control When Device Configuration Files are Purged from the Database, on page 116.)

View Archived Files for a Specific Device

Note If you only see a running configuration file and not a startup file, that is because the two files are the same. Cisco Evolved Programmable Network Manager only backs up the startup configuration when it is different from the running configuration.

Step 1 Choose **Inventory** > **Device Management** > **Configuration Archive**, then click the **Devices** tab.

Step 2 Click a device name hyperlink. Cisco Evolved Programmable Network Manager lists archived files according to their timestamps.

View the Raw Content of an Archived Configuration File

Use this procedure to view the startup, running, and (if supported) VLAN, database, and admin configuration files that have been saved to the configuration archive. You can choose versions according to timestamps and then compare them with other versions.

Note For Cisco NCS 2000 and Cisco NCS 4000 devices, the database is backed up as a binary file. Because it is not a text file, you cannot view it or compare it with other versions, instead, you can export the file directly.

To view the contents of a running configuration file stored in the configuration archive:

Step 1 Choose **Inventory** > **Device Management** > **Configuration Archive**, then click the **Devices** tab.

Step 2 Click a device name hyperlink. Cisco Evolved Programmable Network Manager lists archived files according to their timestamps.

Step 3 Expand a timestamp to view the files that were archived at that time. You will see the details for Running Configuration, Startup Configuration, Admin Configuration, VLAN Configuration, and Database Configuration. Click the Details hyperlink under these categories, to see more information.

Note If you only see a running configuration file and not a startup file, that is because the two files are the same. Cisco Evolved Programmable Network Manager only backs up the startup configuration when it is different from the running configuration.

Step 4 Click a file under Configuration Type to view its raw data. The Raw Configuration tab lists the file contents, top to bottom.

Step 5 To compare it with another file, click any of the hyperlinks under the Compare With column. The choices depend on the device type and number of configuration files that have been backed up to the archive. Color codes indicate what was updated, deleted, or added.

Label Important Configuration Files With Tags

Assigning tags to configuration files is a clear method for identifying important configurations and convey critical information. The tag is displayed with the list of files on the Configuration Archive page. Tags can also be edited and deleted using the following procedure.

Step 1 Choose **Inventory > Device Management > Configuration Archive**.

Step 2 Under the **Archives** tab, locate the configuration file you want to label, and click **Edit Tag**.

Step 3 Enter your content in the Edit Tag dialog box (or edit or delete existing tags) and click **Save**.

Synchronize Running and Startup Device Configurations

Devices that have startup configuration files and running configuration files may become out-of-sync (unsynchronized). A device is considered out-of-sync if its startup file (which is loaded when a device is restarted) is different from its running configuration. Unless a modified running configuration is also saved as the startup configuration, if the device is restarted, the modifications in the running configuration will be lost. The overwrite operation synchronizes the files by overwriting the device's startup configuration with its current running configuration.

Note This device configuration file synchronize operation is different from the Sync operation, which performs *an immediate inventory collection for a device*. That Sync operation is described in Collect a Device's Inventory Now (Sync), on page 449.

Step 1 Identify the devices that are out-of-sync:

a) Choose **Inventory > Device Management > Configuration Archive**.

b) Under the **Devices** tab, check the **Startup/Running Mismatch field** .

c) If any devices list **Yes**, make note of the devices.

Step 2 To synchronize the devices:

a) Under the **Devices** tab, select the out-of-sync devices, and click **Schedule Archive Overwrite**. (See Overwrite a Startup Configuration with a Running Configuration, on page 124 for more information about the overwrite operation.)

Step 3 To check the job details, choose **Administration > Job Dashboard** to view details about the overwrite jobs.

Download Configuration Files

You can download the Startup and Running configuration files of up to a maximum of 1000 devices at a time, to your local system.

Step 1 Choose **Inventory > Device Management > Configuration Archive**.

Step 2 In the **Export Latest Archives** drop-down list, select one of the following options to download the configuration files:

a. **Sanitized**—The device credential password will be masked in the downloaded file.

b. **Unsanitized**—The device credential password is visible in the downloaded file.

The Unsanitized option appears based on the user permission set in Role Based Access Control (RBAC).

This option downloads all supported configuration in the device as a csv file. To download only the Startup or the Running configuration in the device, use the alternate steps given below:

- Click the device for which you want to download configuration files in the **Inventory > Device Management > Configuration Archive** page or Click the device for which you want to download configuration files in the **Inventory > Device Management > Network Devices** page and click **Configuration Archive** tab.
- Use the expand icon to display the required configuration details in the archive.
- Click **Details**.
- Select **Sanitized** or **Unsanitized** in the **Export** drop-down list.

Remember Before you upload this config file to your WLC, you must add a keyword, **config** at the beginning of each line.

Compare or Delete Device Configuration Files

The comparison feature displays two configuration files side by side with additions, deletions, and excluded values indicated by different colors. You can use this feature to view the differences between startup and running configuration files for out-of-sync devices, or to find out if similar devices are configured differently. You can then delete the configuration archives from the database.

Cisco Evolved Programmable Network Manager excludes a small set of commands by default, such as the NTP clock rate (which constantly changes on a managed network element but is not considered a configuration change). You can change the excluded commands list as described in Specify Items to be Excluded When Configuration Files Are Checked for Changes, on page 115.

Note File comparisons are not supported on the Cisco NCS 2000 devices because the files are saved in binary format. Only text-based files can be compared.

Step 1 Choose **Inventory > Device Management > Configuration Archive**.

Step 2 To delete the device configuration archive, under the Devices tab, locate the device with the configuration you want to delete and click the X delete button.

Step 3 To compare device configuration archives:

a) Under the Devices tab, locate the device with the configuration you want to compare and click its device name hyperlink.

b) Expand a time stamp to view the files that were archived at that time.

c) Launch a comparison window by clicking any of the hyperlinks under the Compare With column. The choices depend on the device type and number of configuration files that have been backed up to the archive. Color codes indicate what was updated, deleted, or added.

In the Configuration Comparison window, you can peruse the configuration by looking at the raw files or by looking at certain portions of the files (configlets). Use the color codes at the bottom window to find what was updated, deleted, or added.

Deploy an External Configuration File to a Device

The Schedule Deploy operation updates a device's configuration file with an external file. The difference between Rollback and Schedule deploy is that the Rollback uses an existing file from the archive, while Schedule Deploy uses an external file.

Depending on the type of device, you can specify the following settings for the deploy job:

- Overwrite the current startup configuration with the new version and optionally reboot the device after the deploy.
- Merge the new file with the current running configuration and optionally archive the file as the new startup configuration.
- Schedule the deploy of database configuration files in .tgz format.

Note Once the configuration archive deploy is performed from EPNM, you must manually synchronize the device.

Make sure you have the location of the file on your local machine.

Step 1 Open the device's Device Details page, from which you will execute the deploy operation.

a) Choose **Inventory > Device Management > Network Devices**.

b) Click the device name hyperlink to open the Chassis View.

Step 2 Open the Configuration Archive page of the device by clicking the **Configuration Archive** tab.

Step 3 Click **Schedule Archive Deploy** to open the **Schedule Deploy** dialog box.

Step 4 Browse the file you want to deploy by clicking the **Choose file** button.

Note To deploy the database configuration files on Cisco for NCS 4000 devices, you must upload the files in **.cfg** format.

Step 5 Expand the **Scheduling Options** drop-down, and schedule the deployment by choosing the **Start Time**.

Step 6 Configure the job parameters, depending on the type of file you are deploying:

- Startup configuration—Choose **Overwrite Startup Configuration**. If you want to reboot the device after the deploy operation, check the **Reboot** check box.
- Running configuration—Choose **Merge with Running Configuration**. If you want to also save the file on the device as the startup configuration, check the **Save to Startup** check box.
- Database configuration—Choose **Deploy Database Configuration** and select a database file.
- Admin configuration—Choose **Merge with Admin Configuration** and enter the **Device VM Admin Password**.

Step 7 Schedule the deploy job to run immediately or at a future time, and click **Submit**.

Step 8 Choose **Administration > Job Dashboard** to view details about the schedule deploy job.

Overwrite a Startup Configuration with a Running Configuration

The overwrite operation copies a device's running configuration to its startup configuration. If you make changes to a device's running configuration without overwriting its startup configuration, when the device restarts, your changes will be lost.

Note Do not use the **Schedule Archive Overwrite** button in the Devices tab (shown when you choose **Inventory** > **Device Management** > **Configuration Archive**) because it only allows you to select a device but not select a configuration file.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 Click the device name hyperlink to open the device's details page, then click the Configuration Archive tab.

Cisco Evolved Programmable Network Manager

Step 3 Click **Schedule Archive Overwrite** and set the job to run immediately or at a future time, then click **Submit**.

Step 4 Choose **Administration > Job Dashboard** to view the image activation job.

Roll Back a Device's Configuration To an Archived Version

The rollback operation copies files in the archive to devices, making the new files the current configuration. You can roll back running, startup, and VLAN configurations. By default, the operation is performed by merging the files. If you are rolling back a running configuration, you have the option to perform it using overwrite rather than merge. To roll back a configuration file to a previous version.

Step 1 Choose **Inventory** > **Device Management** > **Configuration Archive**.

Step 2 Click the **Archives** tab and check the device that has the configuration file you want to roll back, and click **Schedule Archive Rollback**.

Step 3 Choose the file types that you want to roll back. In the Schedule Configuration Rollback dialog box:

a) Expand the **Rollback Options** area.

b) From the **Files to Rollback** drop-down list, choose the file type. Choosing **All** applies the operation to startup, running, and VLAN configuration files.

Note For Cisco IOS XR 64-bit devices, if you select **Admin Configuration**, enter the **Device VM Admin Password**.

Step 4 Click the specific configuration file version that you want to roll back to.

Step 5 Click **Schedule Archive Rollback** and complete the following:

Table 11: Roll Back Device Configuration

Area	Option	Description
Rollback	Files to rollback	Select Database Configuration, Running Configuration, or Admin Configuration.
	Reboot	(Startup only) After rolling back the startup configuration, reboot the device so the startup configuration becomes the running configuration.
	Save to startup	(Running only) After rolling back the running configuration, save it to the startup configuration.
	Archive before rollback	Back-up the selected file(s) before beginning the rollback operation.
	Overwrite configurations	Overwrite (rather than merge) the old running configuration with the new one.
	Continue rollback on archive failure	(If Archive before rollback is selected) Continue the rollback even if the selected files are not successfully backed up to the database.
	VRF Name	Select the applicable VRF name from the drop-down list. The VRF name is validated on submission.
Rollback	Rollback Database Configuration	Begin the rollback operation for database configuration files.
Schedule	(see web GUI)	Specify whether to perform the rollback immediately or at a later scheduled time.

Step 6 Click **Submit**.

Export Configuration Files to a Local File System

You can export running configuration files and startup configuration files.

Note For Cisco NCS 2000 devices, you can export database configurations as binary files to a file system on your local machine. With Cisco NCS 4000 devices, you can export database configurations as .tgz files. When you export it, your browser will prompt you to save or open the file.

Step 1 Choose **Inventory** > **Device Management** > **Configuration Archive**.

Step 2 Under the Devices tab, locate the device with the archive you want to export, and click its device name hyperlink.

Step 3 Locate the configuration version you want to export and expand it.

Step 4 Under the Configuration Type column, click the hyperlink for the file you want to export (**Running Configuration** or, if supported, **Startup Configuration**, or **Database Configuration**).

Step 5 In the file viewer page, click **Export** and save the file to your local machine.

Delete Archived Device Configuration Files

Provided you are a user who has the device configuration rollback privilege, you can complete one of the following procedures to manually delete archived device configuration files from the database.

(Method 1)

1. Choose **Inventory** > **Device Management** > **Configuration Archive**.

   The **Configuration Archive** page opens with the **Devices** tab selected.

2. From the **Name** column, click the link for the device whose configuration files you want to delete.

   Its **Archive Details** page opens.

3. Click the radio button for the configuration files you want to delete and then click the **X** (**Delete**) icon.

4. Click **Yes** to confirm deletion of the configuration files.

(Method 2)

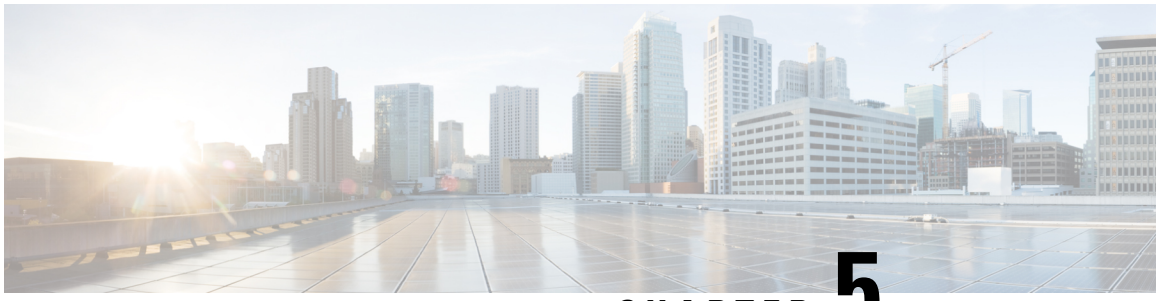
1. Choose **Inventory** > **Device Management** > **Configuration Archive**.

   The **Configuration Archive** page opens with the **Devices** tab selected.

2. Click the **Archives** tab.

3. Check the check box for the configuration files you want to delete and then click the **X** (**Delete**) icon.

4. Click **Yes** to confirm deletion of the configuration files.



CHAPTER 5

Manage Device Software Images

Set Up Software Image Management

Note IPv6 support is not available.

Make Sure Devices Are Configured Correctly

Cisco Evolved Programmable Network Manager can transfer files to and from devices only if the SNMP read-write community strings configured on your devices match the strings that were specified when the devices were added to Cisco Evolved Programmable Network Manager. In addition, devices must be configured according to the settings in How Is Inventory Collected?, on page 52.

Note To improve security, Cisco Evolved Programmable Network Manager no longer uses some of the SSH CBC (Cipher Block Chaining) ciphers that older Cisco IOS-XE and IOS-XR versions use, as they have been deemed weak. For devices running Cisco IOS-XE, ensure that you upgrade to version 16.5.x or later. And for devices running Cisco IOS-XR, upgrade to version 6.1.2 or later. Otherwise, several Software Image Management operations will fail.

Although we do not recommend doing so (since it weakens security), you also have the option to add the CBC ciphers that Cisco Evolved Programmable Network Manager stopped using back to its SSHD service configuration file. To do so, first configure the CBC ciphers in the ciphers line of the file located in the **/etc/ssh/sshd_config** directory (as shown in the example below), then restart the sshd service using the **service sshd stop/start** command.

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,
arcfour256,arcfour128,aes128-cbc,3des-cbc,
cast128-cbc,aes192-cbc,aes256-cbc
```

Note Software Image Management is not supported in the NAT environment. This means that image management features such as image import, upgrade, distribution, and activation, will not function in the NAT environment.

Verify the FTP/TFTP/SFTP/SCP Settings on the Cisco Evolved Programmable Network Manager Server

If you will be using FTP, TFTP, SFTP, or SCP make sure that it is enabled and properly configured. See Enable FTP/TFTP/SFTP Service on the Server, on page 767.

How to Control Images that are Saved to the Image Repository During Inventory Collection

Because collecting software images can slow the data collection process, by default, Cisco Evolved Programmable Network Manager does not collect and store device software images in the image repository when it performs inventory collection. Users with Administration privileges can change that setting using the following procedure.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Image Management**.

Step 2 To retrieve and store device images in the image repository when Cisco Evolved Programmable Network Manager performs inventory collection, check the **Collect images along with inventory collection** check box.

Step 3 Click **Save**.

Adjust Image Transfer and Distribution Preferences

Use this procedure to specify the default protocols Cisco Evolved Programmable Network Manager should use when transferring images from the software image management server to devices. You can also configure Cisco Evolved Programmable Network Manager to perform, by default, a variety of tasks associated with image transfers and distributions—for example, whether to back up the current image before an upgrade, reboot the device after the upgrade, continue to the next device if a serial upgrade fails, and so forth. Users with Administration privileges can change that setting using the following procedure.

This procedure only sets the defaults. You can override these defaults when you perform the actual distribute operation.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Inventory** > **Software Image Management**.

Step 2 On the **Basic** tab, specify the tasks that Cisco Evolved Programmable Network Manager should perform when distributing images:

Setting	Description	Default
Job Preferences		
Continue distribution on failure	If distributing images to multiple devices and distribution to a device fails, continues the distribution to other devices	Enabled
TFTP fallback	Inserts the TFTP fallback command into the running image so that it can be reloaded if image distribution fails Inserts the TFTP fallback command into the running image so that it can be reloaded if image distribution fails	Disabled
Backup running image	Before image distribution, backs up the running image to the TFTP server	Disabled
Insert boot command	Inserts the boot command into the running image, after image distribution	Disabled
Smart Flash Delete Before Distribution	Delete the unnecessary files from flash to free up the memory space before distribution	Disabled
Other Preferences		
Collect images along with inventory collection	Choose this option if you want the software image to be collected from the device and store in the image repository during inventory collection.	Disabled
Show latest images for the available major releases	Choose this option if you want to view the latest maintenance release.	Disabled
Show images with same feature support	Choose this option if you want to view the available images with the same features supported by the running image.	Disabled

Setting	Description	Default
Show available higher image versions	Choose this option if you want to view the available higher image versions for the running image.	Disabled
Remove the option to activate software during distribution jobs	Choose this option to remove the option to activate the software during distribution jobs.	Disabled
Copy operation to be initiated by the EPN Manager server	Choose this option if you want the copy operation to be initiated by the EPN Manager server.	Disabled

Step 3 Specify the default protocol Cisco Evolved Programmable Network Manager should use when transferring images in the Image Transfer Protocol Order. Arrange the protocols in order of preference. If the first protocol listed fails, Cisco Evolved Programmable Network Manager will use the next protocol in the list.

Note When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP for the image distribution, ensure that the device is managed in Cisco Evolved Programmable Network Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

Step 4 Click **Save**.

Add a Software Image Management Server to Manage Groups of Devices

To distribute images to a group of devices, add a software image management server and specify the protocol it should use for image distribution. You can add a maximum of three servers.

Step 1 Add the server.

a) Choose **Administration** > **Servers** > **Software Image Management Servers**.
b) Click the Add Row icon and enter the server name, IP address, and device group the server will support.
c) Click **Save**.

Step 2 Configure the server protocol settings.

a) Check the check box next to the server name, then click **Manage Protocols**.
b) Click the Add Row icon and enter the software image management protocol details (username, password, and so forth).
c) Click **Save**.

Copy Software Images from Devices to the Image Repository (Create a Baseline)

Depending on your system settings, Cisco Evolved Programmable Network Manager may copy device software images to the image repository during inventory collection (see How to Control Images that are Saved to the Image Repository During Inventory Collection, on page 128). If you need to perform this operation manually, use the following procedure, which imports software images directly from devices into the image repository.

Before you begin, ensure that images are physically present on the devices (rather than remotely loaded).

Note If you are importing many images, perform this operation at a time that is least likely to impact production.

Step 1 Choose **Inventory** > **Device Management** > **Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog box, complete the following:

a) In the **Source** area, select the devices (you may want to select one device group at a time).

b) In the **Collection Options** area, specify whether to import the files immediately or schedule the import for later.

Step 4 Click **Submit**.

How Do I Find Out Which Images Are Used by Network Devices?

To view a list of the images used by network devices, choose **Reports** > **Reports Launch Pad** > **Device** > **Detailed Software**.

To list the top ten images use by network devices (and how many devices are using those images), choose **Inventory** > **Device Management** > **Software Images**. Click **Software Image Repository** under **Useful Links**, then then click the **Image Dashboard** icon in the top-right corner of the page.

How Do I Know a Device Has the Latest Image?

If your device type supports image recommendations, you can use the following procedure to check if a device has the latest image from Cisco.com. Otherwise, use the Cisco.com product support pages to get this information.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**, then click the device name hyperlink to open the Device Details page.

Step 2 Click the **Software Image** tab and scroll down to the Recommended Images area. Cisco Evolved Programmable Network Manager lists all of the images from Cisco.com that are recommended for the device.

Cisco Evolved Programmable Network Manager

Note The recommendations list is purely informational. To use any of the recommended images, you must get them from Cisco.com and add them to the image repository. See Add (Import) Software Images to the Repository, on page 133.

View the Images That Are Saved in the Image Repository

Use this procedure to list all the software images saved in the image repository. The images are organized by image type and stored in the corresponding software image group folder.

Step 1 Choose **Inventory** > **Device Management** > **Software Images**. Cisco Evolved Programmable Network Manager lists the images that are saved in the image repository within the **Software Image Summary** panel.

From here you can:

- Import new images into the image repository from network devices; file systems on client machines, IPv4 or IPv6 servers (URLs), FTP servers, and Cisco.com. You can use the web GUI to find out what images are available from Cisco.com, but images must be manually downloaded and then imported. See Add (Import) Software Images to the Repository, on page 133.
- Adjust the requirements that a device must meet in order to upgrade to this image. See Change the Device Requirements for Upgrading a Software Image, on page 136.
- Perform an upgrade analysis. See Verify That Devices Meet Image Requirements (Upgrade Analysis), on page 136.
- Copy new software images to devices. See Distribute a New Software Image to Devices, on page 137.
- Activate images, which makes a new image the device's running image. See Activate a New Software Image on Devices, on page 143.
- Commit Cisco IOS XR images, which persists the image across device reloads and creates a rollback point. See Commit Cisco IOS XR Images Across Device Reloads, on page 148.
- Delete images from the image repository (images can only be deleted using the manual process). See Delete Software Image Files from the Image Repository, on page 149.

Step 2 Go to Software Image repository and click a software image hyperlink to open the Image Information page that lists the file and image name, family, version, file size, and so forth.

From here you can:

- See which devices are using this image by checking the Device Details area at the bottom of the page.
- Adjust the requirements that a device must meet in order to upgrade to this image. (See Change the Device Requirements for Upgrading a Software Image, on page 136.)

Note Version information is captured from the image name. For example, if the image name is *asr9k-mgbl-px-6.8.2* (EPNM supported format), then the version is shown as 6.8.2. For ASR9k 64-bit images with format *asr9k-services-x64-1.0.0.0-r761*, version is displayed as the build version, that is, 1.0.0.0.

Find Out Which Devices Are Using an Image

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 In the **Software Image Summary** panel, locate the image that you are interested in by expanding the image categories in the navigation area or entering partial text in one of the Quick Filter fields. For example, entering **3.1** in the Version field would list Versions 3.12.02S, 3.13.01S, and so forth.

Step 3 Click the image hyperlink to open the Software Image Summary page. Cisco Evolved Programmable Network Manager lists all devices using that image in the Device Details area.

How Do I Know Whether I have Permission to Download Software from Cisco.com

Cisco EPN Manager displays the recommended latest software images for the device type you specify, and it allows you to download the software images directly from Cisco.com. In order to download a EULA or K9 software image from Cisco.com, you must accept/renew the EULA agreement or K9 Agreement periodically.

Cisco EPN Manager does not display deferred software images. For detailed information, see the Cisco EPN Manager 2.1 Supported Devices list.

Add (Import) Software Images to the Repository

Cisco EPN Manager displays the recommended latest software images for the device type that you specify.

Note To download a K9 software image from cisco.com, you must accept/renew the https://software.cisco.com/download/eula.html K9 agreement periodically.

The following topics explain the different ways that you can add software images to the image repository. For an example of how to troubleshoot a failed import, see Manage Jobs Using the Jobs Dashboard, on page 23.

- Add a Software Image That Is Running on a Managed Device, on page 134
- Add a Software Image from an IPv4 or IPv6 Server (URL), on page 134
- Add a Software Image for an FTP Protocol Server (Protocol), on page 135
- Add a Software Image from a Client Machine File System, on page 135

Note For Cisco NCS and Cisco ONS devices, you can only import software images using the procedure given in Add a Software Image from a Client Machine File System, on page 135.

Add a Software Image That Is Running on a Managed Device

This method retrieves a software image from a managed device and saves it in the image repository.

Note When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring very large files or when the server and client are geographically distant from each other. If you choose SCP for the image distribution, ensure that the device is managed in Cisco Evolved Programmable Network Manager with full user privilege (Privileged EXEC mode); otherwise the distribution will fail due to copy privilege error (SCP: protocol error: Privilege denied).

Note that TFTP is supported only when copying images from the device to the server and not the other way around.

Limitations:

- For Cisco IOS-XR devices, direct import of images from the device is not supported by Cisco Evolved Programmable Network Manager; SMU and PIE imports are also not supported on these devices.
- For Cisco IOS-XE devices, if the device is loaded with the 'packages.conf' file, then images cannot be imported directly from that device.

Step 1 Choose **Inventory** > **Device Management** > **Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog:

a) Click **Device** and under Collection Options, choose one or more devices.
b) Select the **VRF Name** check-box and specify the VRF name if you want to enable collection via VRF.
c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
d) Click **Submit**.

Step 4 To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.

Step 5 Verify that the image is listed on the Software Images page (**Inventory** > **Device Management** > **Software Images**).

Add a Software Image from an IPv4 or IPv6 Server (URL)

You can import software image from network-accessible IPv4 or IPv6 servers. The following file formats are supported: .bin, .tar, .aes, .pie, .mini, .vm, .gz, .ova, .iso, .rpm and .ros.

The file that you import must follow the recommended file naming convention. For example, the naming convention for .tar files is *image family*-*-*image version*.**tar**. Here, the image family must be in capital case. Based on the naming convention, the name for the NCS540.tar file must be **NCS540-iosxr-k9-6.0.2.tar**.

Cisco Evolved Programmable Network Manager supports to import Non-Cisco standard image.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog:

a) Click **URL**.
b) In the URL To Collect Image field, enter a URL in the following format (you can also use an HTTP URL where user credentials are not required):

http://*username***:***password***@***server-ip/filename*

c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
d) Click **Submit**.

Step 4 To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.

Step 5 Verify that the image is listed on the Software Images page (**Inventory** > **Device Management** > **Software Images**).

Add a Software Image for an FTP Protocol Server (Protocol)

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog:

a) Click **Protocol**.
b) Enter FTP in the Protocol field, then enter the FTP user name, password, server name or IP address, and file name. The following is a file name example:

/*ftpfolder*/asr901-universalk9-mz.154-3.S4.bin

c) In the Schedule area, schedule the job to run immediately, at a later time, or on a regular basis.
d) Click **Submit**.

Step 4 To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.

Step 5 Verify that the image is listed on the Software Images page (**Inventory > Device Management > Software Images**).

Add a Software Image from a Client Machine File System

Before you begin

When you import the software image file, the browser session is blocked temporarily. If the upload operation exceeds the idle timeout limit of the browser session, then you will be logged out of Cisco Evolved Programmable Network Manager and the file import operation will be aborted. So it is recommended that you increase the idle timeout limit before you begin with this import operation. To increase the idle timeout, see Configure the Global Timeout for Idle Users, on page 814.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the **Add/Import** icon.

Step 3 In the Import Images dialog:

a) Click **File**.
b) Click the **Browse** button and navigate to the software image file.
c) In the Schedule area, schedule the job to run immediately, later, or on a regular basis.

d) Click **Submit**.

Note You must use the URL or Protocol options to import files of larger size (say, greater than 200 MB), as importing through the File option is not recommended.

Step 4 To view the status of the job, click the job link in the pop-up message or choose **Administration > Job Dashboard**.

Step 5 Verify that the image is listed on the Software Images page (**Inventory > Device Management > Software Images**).

Change the Device Requirements for Upgrading a Software Image

Use this procedure to change the RAM, flash, and boot ROM requirements that a device must meet for a software image to be distributed to the device. These values are checked when you perform an upgrade analysis (see Verify That Devices Meet Image Requirements (Upgrade Analysis), on page 136).

Note This operation is not supported on the Cisco NCS 2000 and Cisco ONS families of devices.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 In the **Software Image Summary** panel, locate and select the software image by clicking its associated hyperlink.

Step 3 Click the software image name hyperlink to open its image information.

Step 4 Adjust the device requirements:

- Minimum RAM (from 1 – 999999999999999)
- Minimum FLASH (from 1 – 999999999999999)
- Minimum Boot ROM Version

Step 5 Click **Save**.

Step 6 Click **Restore Defaults**, if you want to retain the previous requirements.

Verify That Devices Meet Image Requirements (Upgrade Analysis)

An upgrade analysis verifies that the device contains sufficient RAM or FLASH storage (depending on the device type), verifies if the image is compatible with the device family and if the software version is compatible with the image version running on the device. After the analysis, Cisco EPN Manager displays a report that provides the results of a device. The report data is gathered from:

- The software image repository, which contains information about minimum RAM, minimum Flash, and so on, in the image header.
- The Cisco EPN Manager inventory, which contains information about the active images on the device, flash memory, modules, and processor details.

Note Upgrade analysis is supported on all Cisco IOS-XR devices (such as Cisco NCS 1000 series, Cisco NCS 4000 series, Cisco NCS 5000 series, Cisco NCS 5500 series, and Cisco NCS 6000 series), except on Cisco ASR 9000 devices and Cisco NCS 1010 devices.

If you want to adjust the device requirements for an image, see Change the Device Requirements for Upgrading a Software Image, on page 136.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click **Upgrade Analysis** under **Useful Links** (do not select an image from the Software Images page).

Step 3 In the Upgrade Analysis dialog:

a) Choose the source for the software images (the image repository or Cisco.com).
b) Select the devices that you want to analyze.
c) Select the software images that you want to analyze the devices against.
d) Click **Run Report**.

The report groups devices by their IP address.

Distribute a New Software Image to Devices

The image distribution operation copies a new software image to a specified location on a device. You can distribute images for similar devices in a single deployment, adjusting your choices per device. When you create the job, you determine whether the job runs immediately or at a scheduled time.

Note Cisco EPN Manager does not use TFTP to distribute images from a server to devices.

When you select an image to be distributed, Cisco EPN Manager only displays devices that are suitable for the image. When you create the distribution job, you specify whether Cisco EPN Manager should:

- Activate the image in the same job or skip the activation. Delaying the activation lets you perform these tasks before activating the image.
  - Find out if there is insufficient memory, clear the disk space for distributing the image or package.
  - Do an upgrade analysis to check the suitability of the device for the chosen image.
- (Cisco IOS-XR only) Commit the image in the same job or skip the commit.

Limitations:

- When you distribute an image to Cisco IOS-XR devices (except Cisco ASR 9000 series devices), the image is copied to the device storage before the install package is activated and committed. With Cisco ASR 9000 series devices, however, the image is install-added on the device directly from Cisco EPN Manager without being copied to the device storage. This reduces the space consumed by the images on the devices. Use the following command to move the image to inactive state instead of copying the image to the device storage:

  `install add protocol://image path/image name`

- For Cisco ASR 9000 devices, only upto 16 device-package pairs can be activated at the same time. Also, the activation of the *.tar* images must contain the same maximum number of packages.
- During the distribution process, if the protocols used for distribution are not supported by the device, then distribution may fail. For example, if you use the SCP protocol to distribute an image to Cisco ASR 9000 series devices, then the distribution fails, because copy of the image onto the device storage is not supported in the device's command line.
- Cisco EPN Manager supports up to five active Distribute operations in parallel. These Distribute operations will not include the Active operations.

The image can be distributed to any file system on the device, including folders in the root directory. This is supported only for Cisco NCS 4200 series devices, Cisco NCS 520 series devices(IOS-XE), and Cisco ASR 907 routers. If you choose a file system that has a standby flash, then the image is distributed to the active flash and the standby flash. This means that when you choose to distribute the image to active flash, you are not required to re-distribute the image to the standby flash.

Note The option to distribute an image directly to a device folder is supported only on Cisco ASR 907 routers and Cisco NCS 4200 series devices.

Cisco EPN Manager displays feedback and status as the operation proceeds. If you are distributing an image to many devices, you can stagger reboots so that the service at a site is not down during the upgrade window. For image distribution to work efficiently, the device and server from which the distribution is performed must be in the same geographical location or site. The distribution job returns an error if the distribution takes more time due to slow network or low speed.

Before You Begin

- When distributing an image to a device, use the most secure protocols supported by the device (for example, SCP instead of TFTP). TFTP tends to time out when transferring large files or when the server and client are geographically distant from each other. If you choose SCP protocol for the image distribution, ensure that the device is managed in Cisco Evolved Programmable Network Manager with full user privilege (Privileged EXEC mode); otherwise the distribution fails due to copy privilege error (SCP: protocol error: Privilege denied).
- When distributing images to Cisco ME 1200 devices, you will need to activate the image on the device immediately after distribution. Ensure that the device is ready for an image activation.

Step 1 Choose **Inventory** > **Device Management** > **Software Images**.

Step 2 Click the blue **Distribute** icon in the Software Image Management Lifecycle widget. Cisco EPN Manager displays the devices that are appropriate for the images. You can configure the image for each device when you create a distribution job.

Note If the required device is not listed here, ensure that the Image Family associated with the file is same as the selected device's family.

To verify the device family, type, version, and size, use the **Image** tab in the Device Details page.

Step 3 From the **Image Selection** tab, select the image that you want to distribute on devices.

Note View the Image family, type, version, and size details for the selected image.

Step 4 From the **Device Selection** tab, select the devices for image distribution. You can further adjust the distribution settings for each device.

Step 5 From the **Image Details Verification** tab, select the file system on the device where the image must be distributed using the **Distribute Location** drop-down menu. This field displays the folders available on the device. To distribute the image to new folders, create the folder on the device manually, and return to this step. Alternatively, you can create a new folder during the distribution process automatically by choosing the 'swim_configuration.xml' file under *'/opt/CSCOlumos/swim'* and providing any new folder name of your choice. The folder is automatically created under this directory. The **Verification State** field displays the status of the software chosen. Based on the status (Success or Failure) you can decide on the compatibility state of the device chosen. For example, if the state is success, then there is enough space to proceed with the distribution of an image.

a) In the **Image Details Verification** tab, Cisco EPN Manager displays one row per device and image.

b) For each device, check the location where the image will be copied. Cisco EPN Manager chooses the location based on its memory calculations.

Note Locations are not supplied for the Cisco NCS 2000 series and Cisco ONS devices.

To change the location, double-click the location value in the **Distribute Image** field and choose another location from the drop-down list.

After you click **Save**, Cisco EPN Manager calculates whether the location has adequate space for the image. If there is enough space, Cisco EPN Manager displays a green check mark (after you click **Save**).

Otherwise, you must choose another location, or select the **Smart Flash Delete Before Distribution** option given in step 6. Running images are not deleted from the device.

Step 6 Configure the distribution settings.

In the **Image Deployment** tab area, configure the behavior for the distribution job—for example, in a bulk distribution job, whether to continue the distribution in case of a failure. (The preferences are populated according to defaults set by the administrator. For more information, see Adjust Image Transfer and Distribution Preferences, on page 129.)

For SVO devices:

- If you select a ROADM instance in **Device Selection**, the **Distribute options** available are SVO, Cisco NCS 2000 series devices, and both.
- If you select an OLA instance in **Device Selection**, the **Distribute options** available is Cisco NCS 2000 series devices.

Image Deployment Options:

- **Smart Flash Delete Before Distribution** - Delete any file (other than the running image) to recover disk space in case the device has insufficient memory (additional image files are deleted until adequate space is available in the selected flash).
- **Continue distribution on Failure** - Continue the distribution even if it fails on a device.

- **TFTP Fallback** - Reload an image if the distribution fails by inserting the TFTP failback command into the running image.
- **Insert Boot Command** - Insert the boot command into the running image after the image is distributed.
- **ISSU** - Activate In-Service Software Upgrade (ISSU) to update the software on the device with minimal service interruption.
- **Upgrade FPD Image** - Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. Select this option to automatically choose FPD image packages for the upgrade during image distribution and activation processes. Additional features include:
  - Smart Flash Delete Before Distribution
  - Parallel Distribution
  - Continue distribution on failure
- **Interface Module Delay** - Adjusts the delay between the Online Insertion and Removal (OIR) of each Interface Module (IM).
- **Erase Running Image** - Erases the device's running image.
- **Distribute via VRF** - Check the Add Distribute via VRF check box to distribute images through VRF.
  - VRF Name - Enter an appropriate VPN routing and forwarding (VRF) name to be used during distribution of an image and for the file transfer.

    Note This field is available only when the "Distribute via VRF" check box is enabled.

    If multiple devices are selected, only the common VRF Name is displayed in the **VRF Name** field.

Table 12: Support for Image Deployment options

Devices	Smart Flash Delete Before Distribution	Continue distribution on Failure	TFTP Fallback	Insert Boot Command
Cisco IOS (Cisco ASR 901 series routers)	Y	Y	Y	Y
Cisco IOS-XE (Cisco ASR 903 router/Cisco ASR 920 router)	Y	Y	Y	Y
Cisco IOS-XE (Cisco NCS 4200 series devices/Cisco ASR 907 routers)	Y	Y	-	Y
Cisco Nexus devices	Y	Y	Y	Y
Cisco IOS (Cisco ME 36X/Cisco ME 38X devices)	Y	Y	Y	Y

Devices	Smart Flash Delete Before Distribution	Continue distribution on Failure	TFTP Fallback	Insert Boot Command
Cisco IOS-XR devices	Y (for Cisco ASR 9000 series routers, the *.tar* images with version lesser than the running image will be deleted)	Y	-	-
Cisco NCS 2000 series and Cisco ONS 15454 devices	-	Y	-	-
Cisco NCS 4000 series devices	Y	Y	-	-
Cisco NCS 1000 series devices	Y	Y	-	-
Cisco NCS 6000 series devices	-	-	-	-
SVO devices	-	Y	-	-
Cisco NCS 1010 devices	Y	-	-	-

Table 13: Support for Image Deployment options

Devices	ISSU	Upgrade FPD Image	Interface Module Delay	Erase Running Image	Distribute via VRF
Cisco IOS (Cisco ASR 901 routers)	-	-	-	-	Y
Cisco IOS-XE (Cisco ASR 920 routers)	-	-	-	-	Y
Cisco IOS-XE (Cisco NCS 4200 series devices/Cisco ASR 903 routers, Cisco ASR 907 routers)	Y (only if device is in 'Install' mode)	-	Y (only if ISSU is available)	-	Y
Cisco Nexus devices	-	-	-	-	-
Cisco IOS (Cisco ME 36X devices/Cisco ME 38X devices)	-	-	-	Y	-
Cisco IOS-XR devices	Y (only for Cisco NCS 4000 series devices, Cisco ASR 9000 32-bit routers,and Cisco NCS 560 series devices)	-	-	-	-

Devices	ISSU	Upgrade FPD Image	Interface Module Delay	Erase Running Image	Distribute via VRF
Cisco NCS 2000 series and Cisco ONS 15454 devices	-	-	-	-	-
Cisco NCS 4000 series devices	Y	Y	-	-	-
Cisco NCS 1000 series devices	-	Y	-	-	-
Cisco NCS 6000 series devices	-	-	-	-	-
Cisco NCS 1010 devices	-	Y	-	-	Y

Step 7 In the **Activate Job Options** window, choose the required settings as applicable:

- Activate Options: Sequential or Parallel
- Continue on failure: Continue the distribution even if it fails on a device.
- Commit: Commit the image on the device post distribution.
- FPDs Upgrade: Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. If you enable this option, FPD image packages will be used for the upgrade.

Step 8 Configure the image activation settings.

Device OS	Settings
Cisco IOS and Cisco IOS-XE	Check **Insert Boot Command** if you want the image to be activated when the device reloads, and: • If you *do* want to reload the device at the end of the operation (and activate the image)—choose **Sequential**, or **Parallel** from the drop-down list. This option is not available for Cisco IOS-XE devices. • If you *do not* want to reload the device at the end of the operation—Choose **OFF** from the drop-down list. If you did not check Insert Boot Command but you want to activate the image, choose **Sequential** or **Parallel**.
Cisco IOS-XR, Cisco NCS 2000 series devices, and Cisco ONS	• If you *do* want to activate or reload the image, choose either **Sequential** or **Parallel** from the drop-down list. • If you *do not* want to activate the image, choose **OFF** from the drop-down list. **Note** If you choose to perform an ISSU upgrade, choose **OFF** from the drop-down list. This option is only applicable to some Cisco IOS-XR devices such as Cisco NCS 4000 series, Cisco ASR 9000 32-bit routers, and Cisco NCS 560 devices. **Note** If you choose **OFF** from the drop-down list, the **Only image downgrade** option is disabled. This option is applicable to all Cisco NCS 2000 series devices.

The activation options are sometimes hidden because the ability to activate images during the distribution process has been disabled in the Admin settings. To activate images, please return to **Inventory > Device Management > Software Images** and click the **Activate** icon.

Step 9 (Cisco IOS-XR devices) Configure the image commit settings. To commit the image in this job, check **Commit**. If you want to commit the image later, do not check **Commit** and then use the procedure in Commit Cisco IOS XR Images Across Device Reloads, on page 148.

Step 10 In the Schedule Distribution area, schedule the job to run immediately, later, or regularly.

Step 11 Click **Submit**.

Step 12 Choose **Administration > Job Dashboard** to view details about the image distribution job.

Note If the copy task takes longer than two hours, verify your connection speed from Cisco EPN Manager to the selected device.

What to do next

If you encounter the following image distribution error, please configure the device with the commands listed, and try again:

Problem: You encounter the error- 'ssh connections not permitted from this terminal'.

Cause: Device is configured incorrectly.

Solution: Configure the device with the following commands

```
line vty 0 <number available in the device>
               transport input ssh
               transport output ssh
```

<number available in the device> -represents the unique identifier that varies from 15 to over 100 depending on the IOS version running on the device.

Note These commands are not supported on Cisco IOS-XR devices.

Activate a New Software Image on Devices

Note To activate Cisco IOS-XR images, you can use this procedure or the procedure given in Activate, Deactivate, and Remove Cisco IOS XR Images from Devices, on page 146 (which performs the deactivate operation on single devices).

When a new image is activated on a device, it becomes the running image on the disk. Deactivated images are not removed when a new image is activated; you must manually delete the image from the device.

If you want to distribute and activate an image in the same job, see Distribute a New Software Image to Devices, on page 137.

To activate an image without distributing a new image to a device—for example, when the device has the image you want to activate—use the following procedure. The activation uses the distribution operation but does not distribute a new image.

Note EPNM supports up to 20 active Activate operations in parallel. These Activate operations will not include the Distribute operation.

Before you begin

- Before activating or reverting images on Cisco NCS 2000 devices, ensure that you disable all suppressed alarms on the device.
- If you choose the **ISSU** option to activate an image in Bundle Mode, you can verify if the device is currently in the bundle mode by running this command, **show version | in image** and check if the image has the format: '.bin'. You can also check the format of the image by looking at the filename of the image in the **Image** tab of the Device Details view.
- During activation using the ISSU option, if the device is in subpackage mode, for example, if the image is of the format 'bootflash:ISSU/packages.conf', ensure that you use the same folder to activate the image.

Step 1 Choose **Inventory > Device Management > Software Images**.

Step 2 Click the **Activate** icon in the Software Image Management Lifecycle widget.

Step 3 **Note** You cannot perform the activation operation when the standby version is lower than the active version.

In the **Activation Source** tab, choose **Activate from Library** or **Activate from Completed Distribution Jobs** or **Activate from Standby/Alternate Images** as required.

Step 4 If you choose Activate from Completed Distribution Jobs, go to the **Job selection** tab and select the distributed success or partial success jobs. Then, go to **Activate Preview** tab and select the Device list displayed with the image name and flash details. Click the **Activate Job Options** tab.

Step 5 In the **Activate Job Options** window, choose the required settings and go to Step 10:

- Continue on failure: Continue the activation even if it fails on a device.
- Commit: Commit the image on the device post distribution.
- Insert boot command: Inserts the boot command into the running image after the image is distributed. This is a prerequisite for activating devices with the ISSU option.
- Activate Options: Sequential or Parallel.
- Continue on failure: Continue the distribution even if it fails on a device.
- Commit: Commit the image on the device post distribution.
- FPDs Upgrade: Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. If you enable this option, FPD image packages will be used for the upgrade.
- ISSU options:
  - Device Upgrade Mode: Your options are:

- **Bundle Mode**: If you choose the **ISSU** option to activate an image, choose the Bundle Mode to use a monolithic Cisco IOS image to boot. This ensures that the boot variable of the device pointing to a .bin file gets the device running in the Bundle mode. If you choose this option, you must reload the device after activation. To verify if the device is in bundle mode, run this command **show version | in image** to check if the image is of the format '.bin'. You can also check the format of the image by looking at the filename of the image in the **Image** tab of the Device Details view.
- **Install Mode**: During activation using the ISSU option, use this option if the device is in the subpackage mode, for example, if the image is of the format 'bootflash:/ISSU/packages.conf', the device is running in the Install mode. Ensure that you use the same folder to activate the image. Changing the folder location causes a failure of the activate operation. If you choose the Install Mode for a device which is already running in the Image Mode, the device is activated without reloading (ISSU) and the boot image continues to point to the packages.conf file. In all other scenarios, the devices are reloaded.

  Note Ensure that the current boot variable in the device is 'bootflash:/ISSU/packages.conf' to avoid any duplicate boot variables.

- **Currently Exists**: If you want the device to be activated in the same mode that it is currently operating in (Install or Bundle), choose this option to activate the image using the same mode.

- Interface Module Delay: The time (in seconds) specified in this option adjusts the delay between the Online Insertion and Removal (OIR) of each Interface Module (IM). This option is enabled only when the Insert boot command and the ISSU options are enabled, and when a supported device is selected. It is recommended to set the value of the delay to 1200 seconds or more to provide sufficient time for the upgrade.

Step 6 If you choose Activate from Library in the Activation Source tab, then click the **Image Selection** tab.

Step 7 If you choose Activate from Standby Image, then go to Step 9.

Step 8 In the **Image Selection** tab, choose the software images that you want to distribute.

Step 9 Click the **Device Selection** tab to choose the devices that you want to activate the image.

a) You can click the **Select devices by** toggle button to choose devices from **Group** or **Device** option.
b) If you choose **Group** option, select the Device groups and choose the devices listed under **Choose Devices** pane. The selected devices are listed under the **Selected Devices** pane.

By default, the devices for which the selected image is applicable are shown. For example, if you choose the **Activate from Standby/Alternate Images** option in Step 3, then the Device Selection tab displays only devices such as, Cisco NCS 2000 series devices, Cisco ONS 15454 devices, and Cisco ME1200 devices, which support activation of standby/alternate images.

Step 10 Click the **Activate Image** tab, and verify whether the selected devices and software images are mapped correctly for activation. While using standby images for activation, click the **Verify Images Selection** tab.

Note When you are activating a standby/alternate image, if the version of the standby/alternate image is lower than that of the image running on the device, then the Verification Status Message column displays (in red) that you are downgrading to a lower version.

Step 11 Click the **Activate Job Options** tab, and choose the required Activate Job options.

For ISO-XR devices, if you check the **ISSU** checkbox, stateful switch over will be configured on the devices.

While activating a standby image, if the selected device supports a downgrade, then the **Only image downgrade** check box is displayed. Selecting this check box ensures that the devices are downgraded only if they support the downgrade operation (for example, for Cisco NCS 2000 series devices) and any specified upgrade operation fails.

For SVO devices, choose the devices on which you want to activate the image by selecting **NCS2K** or **SVO** or **Both** from the **Apply to** drop-down list (under **Activation Options**) area.

Step 12 Click **Submit** to activate the software image in the selected devices.

See the table given below for information on Cisco devices and the protocols that they support for image distribution:

Table 14: Cisco Devices and Supported Image Distribution Protocols

Cisco Devices	TFTP	FTP	SCP	SFTP	HTTPS
Cisco ASR 1000 series routers	Yes	Yes	No	Yes	No
Cisco ASR 9000 series routers	Yes	No	No	Yes	No
Cisco IOS-XR (except Cisco ASR 9000 series routers)	Yes	Yes	Yes	Yes	No
Cisco NCS 4200 series, Cisco ASR 900 series routers, or Cisco ASR 1000 series routers	Yes	Yes	Yes	No	No
Cisco ME 1200 devices	Yes	Yes	No	Yes	No
Cisco NCS 2000 series devices and Cisco ONS devices	No	Yes	No	No	Yes
Cisco NCS 1010 devices	Yes	Yes	Yes	Yes	No

Activate, Deactivate, and Remove Cisco IOS XR Images from Devices

You can perform activate, deactivate, and delete operations on specific devices from the **Chassis View** page. That view lists all the running image on the disk.

Before you begin

Before activating or reverting images on Cisco NCS 2000 devices, ensure that you disable all suppressed alarms on the device.

Step 1 Open the **Chassis View** page and click the **Image** tab.

Step 2 Expand the **Applied Images** area to display all the images that are installed on the device.

- Active—Images that devices are actively using.
- Inactive—Images that are added to the boot device but are not activated.
- Available—Images that are physically present on the device but have not been added to the boot device.

Step 3 Use the **Show** drop-down list to filter the list of images on the device. Identify the image that you want to manage, and double-click its Status field. The field changes to an editable row.

Step 4 Choose the operation that you want to perform from the **Status** drop-down list, then click **Save**. . Your options are:

- Active
- Deactivate
- Remove
- Add
- Add and Activate
- Available

Step 5 Click **Apply** above the images table.

Step 6 Choose **Administration** > **Job Dashboard** to view details about the image activation job.

Note Version information is captured from the image name. For example, if the image name is *asr9k-mgbl-px-6.8.2* (EPNM supported format), then the version is shown as 6.8.2. For ASR9k 64-bit images with format *asr9k-services-x64-1.0.0.0-r761*, version is displayed as the build version, that is, 1.0.0.0.

View and Upgrade FPD Images

Field Programmable Devices (FPDs) are hardware devices implemented on router cards that support separate software upgrades. You can configure FPD image packages to be automatically chosen for the upgrade during image distribution and activation processes. Before performing an upgrade, you can view FPD details such as the device name, card type, hardware version, etc.

To do this:

Step 1 Choose **Configuration > Network Devices**.

Step 2 Locate and select the device with the FPD images.

Step 3 Click the **Images** tab.

You can now view the FPD device name, location, available card types and their hardware versions, the ATR values, the status of the image, and the running and programmed values.

Step 4 Once you have reviewed the FPD image details, click the **Upgrade FPD Image** button, to configure the upgrade settings.

Step 5 Schedule the upgrade to run immediately, at a later date and time, or on a regular basis.

Step 6 Click **Submit**.

Commit Cisco IOS XR Images Across Device Reloads

Note For Cisco IOS XR devices, we recommend that you do not commit the package change until the device runs with its configuration for a period of time, until you are sure the change is appropriate.

When you commit a Cisco IOS XR package to a device, it persists the package configuration across device reloads. The commit operation also creates a rollback point on the device which can be used for roll back operations.

If you want to distribute, activate, and commit an image in the same job, use the procedure described in Distribute a New Software Image to Devices, on page 137 .

To commit an activated image, use the following procedure.

Note If you are only working on a single device, perform the commit operation from the Device Details page (click the **Image** tab, choose the image, and click **Commit**).

Step 1 Choose **Inventory** > **Device Management** > **Software Images**.

Step 2 Click the **Commit** icon in the Software Image Management Lifecycle widget.

Step 3 Select the devices with the image you want to commit and click **Submit**. (Images can only be committed if they have been activated.)

Step 4 Select the software image you want to activate, then click **Submit**.

Step 5 In the Schedule Distribution area, schedule the commit job to run immediately, at a later time, or on a regular basis.

Step 6 Click **Submit**.

Step 7 Choose **Administration** > **Job Dashboard** to view details about the image activation job.

Roll Back Cisco IOS XR Images

Rolling back a Cisco IOS XR image reverts the device image to a previous installation state—specifically, to an installation rollback point. If an image has been removed from a device, all rollback points associated with the package are also removed and it is no longer possible to roll back to that point.

A rollback job can only be performed on one device at a time. You cannot perform a rollback for multiple devices in the same job.

Note The rollback feature is only supported on Cisco IOS-XR devices such as Cisco ASR 9000 devices.

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**, then click the device name hyperlink for the device with the image you want to roll back.

Step 2 Click the **Image** tab and expand the Rollback Info area.

Step 3 Select the software image Commit ID you want to roll back to, and click **Rollback**. The Rollback Scheduler opens.

Step 4 If you want to commit the image after the rollback operation completes, check **Commit After Rollback**.

Step 5 In the Schedule Rollback area, schedule the rollback job to run immediately or at a later time, and click **Submit**.

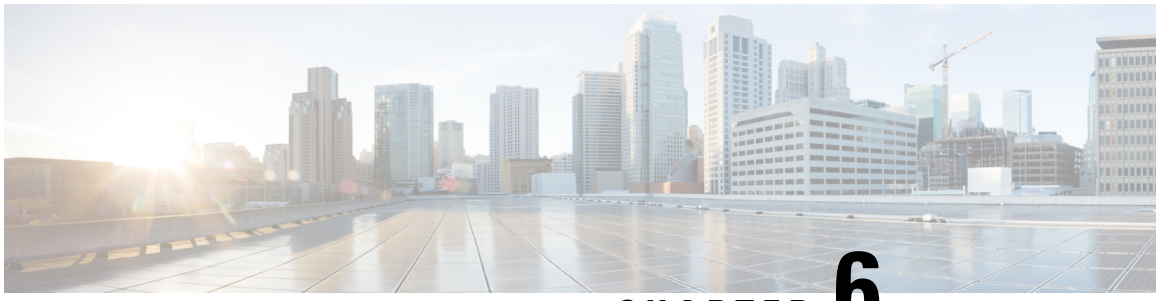
Delete Software Image Files from the Image Repository

Software images can only be *manually* deleted from the image repository; Cisco Evolved Programmable Network Manager does not perform any automatic purging of the image repository. If you have sufficient privileges, you can use the following procedure to delete software image files from the image repository.

Step 1 Choose **Inventory** > **Device Management** > **Software Images**.

Step 2 From the **Software Images Summary** panel on the left, select the images that you want to delete.

Step 3 Click **Delete**.



CHAPTER 6

Perform Configuration Audits Using Compliance

How To Perform a Compliance Audit

The following table lists the basic steps for using the Compliance feature.

	Description	See:
1	Create a *compliance policy* that contains a name and other descriptive text.	Create a New Compliance Policy, on page 152
2	Add rules to the compliance policy. The rules specify what constitutes a violation.	Create Compliance Policy Rules, on page 153

3	Create a *compliance profile* (which you will use to run an audit on network devices) and: • Add a compliance policy to it. • Choose the policy rules you want to include in the audit. You can add multiple custom policies and/or predefined system policies to the same profile.	Create a Compliance Profile That Contains Policies and Rules, on page 157
4	Run a compliance audit by selecting a profile and scheduling an audit job.	Run a Compliance Audit, on page 158
5	View the results of the compliance audit and if necessary, fix the violations.	View the Results of a Compliance Audit, on page 159

Enable and Disable Compliance Auditing

The Compliance feature uses device configuration baselines and audit policies to find and correct any configuration deviations in network devices. It is disabled by default because some of the compliance reports can impact system performance. To enable the Compliance feature, use the following procedure.

Note To use the compliance feature, your system must meet the Professional sizing requirements, as specified in the Cisco Evolved Programmable Network Manager Installation Guide.

Note In Cisco EPN Manager, disabling compliance auditing disables the compliance from GUI and stops the compliance data collection in the background. User must restart the Cisco EPN Manager server and resync the devices for the compliance settings to be functional.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

Step 2 Next to Compliance Services, click **Enable**, then click **Save**.

Step 3 Restart the application.

Step 4 Resynchronize the device inventory: Choose **Inventory**> **Network Devices**, select all devices, then click **Sync**.

Create a New Compliance Policy

You can create a new compliance policy starting with a blank policy template.

Step 1 Choose **Configuration** > **Compliance** > **Policies**.

Step 2 Click the Create Compliance Policy (+) icon in the **Compliance Policies** navigation area on the left.

Step 3 In the dialog box, enter a name and optional description, then click **Create**. The policy is added to the **Compliance Policies** navigation area on the left.

To duplicate the policy, select the policy radio button and click **Duplicate**.

Create Compliance Policy Rules

Compliance policy rules are platform-specific and define what is considered a device violation. A rule can also contain CLI commands that fix the violation. When you are designing the compliance audit job, you can select the rules you want to include in the audit (see Run a Compliance Audit, on page 158).

Cisco EPN Manger supports audit for AireOS Wireless LAN Controllers platform.

Step 1 Choose **Configuration** > **Compliance** > **Policies**, then select a policy from the navigation area on the left.

Step 2 From the work area pane, click **New** to add a new rule.

If a similar rule exists, you can copy the rule by clicking **Duplicate**, editing the rule, and saving it with a new name.

Step 3 Configure the new rule by entering your rule criteria.

Note Cisco Evolved Programmable Network Manager supports all Java-based regular expressions. See http://www.rexegg.com/regex-quickstart.html.

a) Enter a title, description, and other information in the **Rule Information** text fields. This information is free text and does not impact any of the rule settings.
b) Specify the devices for this rule in the **Platform Selection** area.
c) (Optional) In the **Rule Inputs** area, click **New** and specify the input fields that should be displayed to a user when they run a policy that contains this rule. For example, you could prompt a user for an IP address.

Note If you choose the **Accept Multiple Values** check box, the audit will pass only if all the rule inputs match in the condition.

d) In the **Conditions and Actions** area, click **New** and specify the criteria that will be checked. This will determine the rule pass and fail conditions. For examples, see Examples—Rule Conditions and Actions, on page 154.

Step 4 Click **Create**. The rule is added to the compliance policy.

You can create as many rules as you want. Remember that when you want to run the audit job, you can pick the rules you want to validate.

Note It is recommended to use Java regex for testing the expressions while creating a new compliance policy rule and validating a rule or command using regular expressions, if any.

What to do next

Create a profile that contains the compliance policy and its rules, and then perform the audit using the profile. See Create a Compliance Profile That Contains Policies and Rules, on page 157.

Examples—Rule Conditions and Actions

Example Conditions and Actions: DNS Servers Configured on Device

This compliance policy checks if either **IP name-server 1.2.3.4** or **IP name-server2.3.4.5** is configured on the device. If they are, the policy raises a violation with the message "DNS server must be configured as either 1.2.3.4 or 2.3.4.5."

Tab	Tab Area	Field	Value
Condition Details	**Condition Scope Details**	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	ip name-server {1.2.3.4|2.3.4.5}
Action Details	**Select Match Action**	Select Action	Does not raise a violation
	Select Does Not Match Action	Select Action	Raise a violation
		Violation Message Type	User Defined Violation Message
		Violation Text	DNS server must be configured as either 1.2.3.4 or 2.3.4.5

Example: Block Options

This compliance policy checks if there are any rogue or unauthorized SNMP community strings are defined in the given blocks. If they are detected in the blocks, the policy raises a violation with the message *"Detected unauthorized community string <1.1>"* and removes all non-compliant SNMP strings from the blocks.

Tab	Tab Area	Field	Value
Rule Information		Rule Title	snmp-server community having non-standard entries
Platform Selection			Cisco IOS Devices, Cisco IOS-XE Devices
Condition 1			

Condition Details	**Condition Scope Details**	Condition Scope	Configuration
	Block Options	Block Start Expression (This field will be enabled only when Parse as Blocks checkbox is selected)	^snmp-server community .*
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community (.*)
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Does Not Raise a Violation
Condition 2			
Condition Details	**Condition Scope Details**	Condition Scope	Previously Matched Blocks
	Block Options	Block Start Expression (This field will be enabled only when Parse as Blocks checkbox is selected)	^snmp-server community .*
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community ((public RO)|(private RW))
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a Violation
		Violation Message Type	User Defined Violation Message
		Violation Text	Detected unauthorized community string *<1.1>*.

Note In the above example, the matching criteria will be termed as 1.1, 1.2, and so on, for first condition. For the second condition, the matching criterial will be termed as 2.1, 2.2, and so on.

Example Conditions and Actions: Community Strings

This compliance policy checks if either **snmp-server community public** or **snmp-server community private** is configured on a device (which is undesirable). If it is, the policy raises a violation with the message "Community string *xxxxx* configured", where *xxx* is the first violation that was found.

Tab	Tab Area	Field	Value
Condition Details	**Condition Scope Details**	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community {public|private}
Action Details	**Select Match Action**	Select Action	Raise a violation
	Select Does Not Match Action	Select Action	Continue
		Violation Message Type	User Defined Violation Message
		Violation Text	Community string *xxxxx* configured.

Example Conditions and Actions: IOS Software Version

This compliance policy checks if Cisco IOS software version **15.0(2)SE7** is installed on a device. If it is not, the policy raises a violation with the message "Output of show version contains the string *xxxxx*," where *xxxx* is the Cisco IOS software version that does not match 15.0(2)SE7.

Tab	Tab Area	Field	Value
Condition Details	**Condition Scope Details**	Condition Scope	Device Command Outputs
		Show Commands	show version
	Condition Match Criteria	Operator	Contains the string
		Value	15.0(2)SE7
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a Violation
		Violation Message Type	User Defined Violation Message
		Violation Text	Output of show version contains the string *xxxxx*.

Example Conditions and Actions: NTP Server Redundancy

This compliance policy checks if the command **ntp server** appears at least twice on the device. If it does not, the policy raises a violation with the message "At least two NTP servers must be configured."

Tab	Tab Area	Field	Value
Condition Details	**Condition Scope Details**	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	(ntp server.*\n){2,}
Action Details	**Select Match Action**	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a violation
		Violation Message Type	User Defined Violation Message
		Violation Text	At least two NTP servers must be configured.

Create a Compliance Profile That Contains Policies and Rules

A compliance profile contains one or more compliance policies. When you add a compliance policy to a profile, all policy rules are applied to the profile. You can customize the profile by selecting the policy rules that you want to include (and ignoring the others). If you group several policies in a profile, you can check and uncheck the rules for each policy.

If you login as a Root or an Admin user, you will be able to do the following actions:

- Create, edit, or delete a profile.
- Select the rules that are created in the Policies page.

Note "Other" users must enable the following task permissions to perform the relevant actions:

- **Compliance Audit Profile Access** to run the profile, refresh the profile and browse through the policies in the profile.
- **Compliance Audit Profile Edit Access** to create and edit a compliance audit profile.

The task permissions are located in the **Administration** > **Users** > **Users and Roles** > **Roles** page.

If you do not select the **Compliance Audit Profile Access** task permission, you will not be able to view the Profile page, even if you have selected the **Compliance Audit Profile Edit Access** task permission.

Step 1 Choose **Configuration** > **Compliance** > **Profiles**.

Step 2 Click the Create Policy Profile (+) icon in the **Compliance Profiles** navigation area on the left. This opens the **Add Compliance Policies** dialog box.

Step 3 Select the policies that you want to include in the profile. User-defined policies will be available under the User-Defined category.

a) In the **Add Compliance Policies** dialog box, choose the policies you want to add.

b) Click **OK**. The policies are added to the **Compliance Policy Selector** area.

Step 4 Select the rules that you want to include in the policy.

a) Select a policy in the **Compliance Policy Selector** area. The policy's rules are displayed in the area on the right.

b) Select and uncheck specific rules, then click **Save**.

Note The choices you make here only apply to the *policy instance* in *this profile*. Your choices do not modify the original version of the compliance policy.

What to do next

Schedule the compliance audit job as described in Run a Compliance Audit, on page 158.

Import and Export Compliance Audit Profiles

Compliance profiles are saved as XML files. You can import and export individual compliance profiles. Files can be imported only in XML format.

Import Compliance Audit Profiles

Before you import a compliance audit profile, ensure that all user-defined policies associated with the profile are available in Cisco EPN Manager. To import a compliance profile:

1. Navigate to **Configuration** > **Compliance** > **Profiles**.
2. Click the Import Profiles icon in the **Compliance Profiles** area on the left.
3. In the **Import Profiles** dialog box, click **Choose Profiles**.
4. Browse to the profile XML file and select it.
5. (Optional) To import multiple profiles, click **Choose more files** and upload the profile XML files.
6. Click **Import**.

Cisco EPN Manager displays an error message in case an invalid profile XML file is uploaded. Click on the warning icon in the **Import Profiles** dialog to check logs for profiles that failed to import.

Export Compliance Audit Profiles

To export a compliance profile:

1. Hover your mouse on "i" icon next to the profile in the **Compliance Profiles** navigation area on the left.
2. In the **Policy Profile** pop up window, click the **Export Profile as XML** hyperlink, and save the file.

Run a Compliance Audit

To run a compliance audit, select a profile, choose the devices you want to audit (using the policies and rules in the profile), and schedule the audit job.

Step 1 Choose **Configuration** > **Compliance** > **Profiles**.

Step 2 Select a profile in the **Compliance Profiles** navigation area on the left.

Step 3 Click the Run Compliance Audit icon in the **Compliance Profiles** navigation area.

Step 4 Expand the **Devices and Configuration** area, select the required devices and configuration files that you want to audit.

a) Select the devices (or device groups).

b) Specify which configuration file you want to audit.

- **Use Latest Archived Configuration** —Audit the latest backup file from the archive. If no backup file is available,Cisco Evolved Programmable Network Manager does not audit the device.
- **Use Current Device Configuration**— Poll and audit the device's running configuration. (For example, show command output will be from the device's running configuration.)

  When you select this option, Cisco Evolved Programmable Network Manager first takes a backup of the configuration from device and then performs audit. This is useful when periodic or event triggered configuration backup is not enabled and also useful because archived configuration in Cisco Evolved Programmable Network Manager is often out-of-sync with the device.

c) Click **Next**.

Step 5 Enter a value in the **Configure Idle Time Limit (min)** field. By default, the time limit is set to 5 minutes. Users can enter a number between 5 and 30 if they wish to change the time limit. The audit job will be aborted if it is idle for the configured time limit.

Step 6 Select **Now** to schedule the audit job immediately or select **Date** and enter a date and time to schedule it later.

Use the **Recurrence** option to repeat the audit job at regular intervals.

Step 7 Click **Finish**. An audit job is scheduled. A notification pop-up will appear once the audit job is scheduled. To view the status of the audit job, choose **Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs**.

What to do next

Check the audit results as described in View the Results of a Compliance Audit, on page 159.

View the Results of a Compliance Audit

Use this procedure to check an audit job results. The results will tell you which devices were audited, which devices were skipped, which devices had violations, and so forth. There might be several different compliance policies running on a single device.

After a job is created, you can set the following preferences for the job:

- Pause Series—Can be applied only on jobs that are scheduled in the future. You cannot suspend a job that is running.
- Resume Series—Can be applied only on jobs that have been suspended.
- Edit Schedule—Reschedule a job that has been scheduled for a different time.

Step 1 Choose **Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs**.

Step 2 Click the **Audit Jobs** tab, locate your job, and check the information in the **Last Run** column.

Last Run Result Value	Description
Failure	One or more devices audited have a violation in the policies specified in the profile.
Partial Success	The compliance job contains a mix of both audited and non-audited devices, and the compliance status of audited devices is successful.
Success	All devices audited conform to the policies specified in the profile.

For a compliance audit job, the number of violations supported is 20000 for Standard setup and 80000 for Pro and above setup of Cisco Evolved Programmable Network Manager.

Step 3 If the audit check failed:

- To see which devices failed, hover over the "i" icon next to the **Failure** hyperlink to display a details popup.
- Launch a Device 360 view by selecting the job, clicking **View Job Details**, and clicking the "i" icon next to a device in the popup window.

Step 4 For the most detail, click the **Failure** hyperlink to open the **Compliance Audit Violation Details** window.

Note Use the **Next** and **Previous** buttons to traverse the **Compliance Audit Violation Details** window.

What to do next

To fix any of the violations, see Fix Device Compliance Violations, on page 161.

View Violation Job Details

The following table shows the details that can be viewed from the Violation Details page.

To View:	Do the following
The status of scheduled fixable violation jobs.	**1.** Go to the **Violation Details** page. **2.** Click the **Fixable** column filter box and choose **Running**.
The details of Fixed violation jobs.	**1.** Go to the **Violation Details** page. **2.** Click the **Fixable** column filter box and choose **Fixed**. **3.** Click the **Fixed** link.
The details of Fix Failed violation jobs.	**1.** Go to the **Violation Details** page. **2.** Click the **Fixable** column filter box and choose **Fix Failed**. **3.** Click the **Fix Failed** link.

View Audit Failure and Violation Summary Details

You can view detailed violation information, export this data, and view details of compliance jobs. You can export detailed data for a specific job, or export summary data for multiple jobs.

Step 1 Choose **Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs**.

Step 2 To view the details for a specific audit job:

a) Click the **Audit Jobs** tab and locate your job.

b) Click the job's **Failure** hyperlink to view the **Compliance Audit Details** window.

You can view information about the policy name, the set rules, its compliance state, the total violation count, the job's instance count, its highest severity value, and the ignored count values.

c) To export these details use one of the following options:

- To export the violation details to a Microsoft Excel spreadsheet in XLS format, click **Export as XLS**.
- To export the violation details to a Microsoft Excel spreadsheet in comma-separated text, click **Export as CSV**.
- To export the violation details to an HTML file, click Export as HTML.

d) Click **Save File**.

Step 3 To view a collective summary of all audit jobs:

a) Click the **Violation Summary** tab.

You can view a collective report for all devices on which violations have occurred, their associated policy and profile names, their audit job IDs, their associated rules and rule severity values, details on whether the violations are fixable or not, or whether they are already fixed, and the message associated with the violation.

b) To export this detailed summary report, choose one of the following options from the drop-down menu:

- To export the summary to a Microsoft Excel spreadsheet in comma-separated text, click **Violation Report CSV**.
- To export the summary to a PDF file, click **Violation Report PDF**.

c) Click **Save File**.

What to do next

To fix any of the violations, see Fix Device Compliance Violations, on page 161.

Fix Device Compliance Violations

Use this procedure to fix compliance violations for a failed compliance audit.

Step 1 Choose **Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs**.

Step 2 Click the **Audit Jobs**, locate your job, and check the information in the **Last Run Result** column.

Step 3 Click the **Failure** hyperlink to open the **Compliance Audit Violation Details** window.

Note Use the **Next** and **Previous** buttons to traverse the **Compliance Audit Violation Details** window.

Step 4 In the **Job Details and Violations** area, click **Next**.

Step 5 In the **Violations by Device** area, select the device and violation and click **Next**.

Step 6 In the **Fix Rule Inputs** area, preview the fix commands that were previously defined in the policy, then click **Next**.

If custom policies are created with fix CLI ^<Rule input ID>^ as the action for the condition, then the Fix Rule Inputs tab is displayed. Enter the required fix rule values and click **Next** to continue.

Step 7 Review the configuration that is displayed in the Preview Fix Commands pop up.

Step 8 Schedule the fix job so that the generated configuration can be deployed to the device, then Click **Schedule the Fix Job**.

Note User can add the compliance fix CLI to the device's startup configuration. This retains the fix CLI even when the device is rebooted.

What to do next

To view any of the violations job details, see View Audit Failure and Violation Summary Details, on page 161.

View Audit Failure and Violation Summary Details

You can view detailed violation information, export this data, and view details of compliance jobs. You can export detailed data for a specific job, or export summary data for multiple jobs.

Step 1 Choose **Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs**.

Step 2 To view the details for a specific audit job:

a) Click the **Audit Jobs** tab and locate your job.

b) Click the job's **Failure** hyperlink to view the **Compliance Audit Details** window.

You can view information about the policy name, the set rules, its compliance state, the total violation count, the job's instance count, its highest severity value, and the ignored count values.

c) To export these details use one of the following options:

- To export the violation details to a Microsoft Excel spreadsheet in XLS format, click **Export as XLS**.
- To export the violation details to a Microsoft Excel spreadsheet in comma-separated text, click **Export as CSV**.
- To export the violation details to an HTML file, click Export as HTML.

d) Click **Save File**.

Step 3 To view a collective summary of all audit jobs:

a) Click the **Violation Summary** tab.

You can view a collective report for all devices on which violations have occurred, their associated policy and profile names, their audit job IDs, their associated rules and rule severity values, details on whether the violations are fixable or not, or whether they are already fixed, and the message associated with the violation.

b) To export this detailed summary report, choose one of the following options from the drop-down menu:

- To export the summary to a Microsoft Excel spreadsheet in comma-separated text, click **Violation Report CSV**.
- To export the summary to a PDF file, click **Violation Report PDF**.

c) Click **Save File**.

What to do next

To fix any of the violations, see Fix Device Compliance Violations, on page 161.

Import and Export Compliance Policies

Compliance policies are saved as XML files. You can export individual compliance policies and, if desired, import them into another server. Files can only be imported in XML format.

Step 1 Choose **Configuration** > **Compliance** > **Policies**.

Step 2 To export a compliance policy:

a) Mouse hover on "i" icon next to the policy in the **Compliance Policies** navigation area on the left.
b) In the popup window, click the **Export Policy as XML** hyperlink, and save the file.

Step 3 To import a compliance policy:

a) Click the Import Policies icon above the **Compliance Policies** navigation area on the left.
b) In the **Import Policies** dialog box, click **Choose Policies**.
c) Browse to the XML file and select it.
d) Click **Import**.

View the Contents of a Compliance Policy XML File

Compliance policies are saved as XML files. To view the contents of a policy's XML file:

Step 1 Choose **Configuration** > **Compliance** > **Policies**.

Step 2 Locate the policy in the **Compliance Policies** navigation area on the left, then hover your mouse over the "i" icon next to the policy.

Step 3 In the popup window, click the **View Policy as XML** hyperlink. Cisco Evolved Programmable Network Manager displays the content in XML format.

View PSIRT and EOX Information

Note The PSIRT and EOX page displays the PAS and RBML bundle generated dates. The PAS report holds the PSIRT and EoX records that are published on or before the bundle generated dates. It will not display the PSIRT records that are published post the bundle generation.

View Device Security Vulnerabilities

You can run a report to determine if any devices in your network have security vulnerabilities as defined by the Cisco Product Security Incident Response Team (PSIRT). The report includes Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX and Field Notice information. You can also view documentation about the specific vulnerabilities that describes the impact of a vulnerability and any potential steps needed to protect your environment.

Note PSIRT and EOX reports cannot be run for specific devices. When you schedule PSIRT and EOX jobs, the report is generated for all devices in Managed and Completed state (on the **Inventory > Configuration > Network Devices** page).

Before you begin

Sync the devices prior to scheduling the job. Choose **Configuration** > **Network Devices**, select the devices, then click **Sync**.

Step 1 Choose **Reports** > **PSIRT and EoX**.

Step 2 Schedule and run the job. The **Schedule** dialog box appears. You can set the **Start Time** and **Recurrence** options and then click the **Submit** button to schedule the job. Click the **OK** button, in the pop-up that appears, to delete the already scheduled job and create a new one.

A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX and Field Notice information is gathered and reported. Separate jobs on each of the tabs need not be created.

Step 3 Click **View Job Details** to view the current status of the PSIRT report.

Step 4 When the report is completed, click the **Device PSIRT** tab to view PSIRT information.

Step 5 In the **PSIRT Title** column, click the hyperlink to view the full description of a security vulnerability.

Step 6 (Optional) You can export the device PSIRT details in PDF and CSV format for each device and for all devices collectively.

View Device Hardware and Software End-of-Life Report

You can run a report to determine if any Cisco device hardware or software in your network have reached end of life (EOX). This can help you determine product upgrade and substitution options.

Step 1 Choose **Reports > PSIRT and EOX**.

Step 2 Click **Schedule Job**. The **Schedule** dialog box appears. You can set the **Start Time** and **Recurrence** options and then click the **Submit** button to Schedule the job. Click the **OK** button, in the pop-up that appears, to delete the already scheduled job and create a new one.

A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX and Field Notice information is gathered and reported. You do not create separate jobs on each of the tabs.

Step 3 After the job completes, click one of the following EOX tabs to view the report information specific to that tab:

- **Device Hardware EOX**
- **Device Software EOX**
- **Module Hardware EOX**

Step 4 (Optional) You can export these EOX details in PDF and CSV format for each device and for all devices collectively.

View Module Hardware End-of-Life Report

You can run a report to determine if any Cisco module hardware in your network have reached end of life (EOX). This can help you determine product upgrade and substitution options.

Step 1 Choose **Reports > PSIRT and EOX**.

Step 2 Click **Schedule Job**. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX and Field Notice information is gathered and reported. You do not create separate jobs on each of the tabs.

Step 3 Click the **Module Hardware EOX** tab to view the module hardware information.

Step 4 (Optional) You can export these EOX details in PDF and CSV format for each module.

View Field Notices for Device

You can run a report to determine if any Cisco devices that are managed and have completed a full inventory collection have any field notices. Field Notices are notifications that are published for significant issues, other than security vulnerability-related issues, that directly involve Cisco products and typically require an upgrade, workaround, or other customer action.

Step 1 Choose **Reports** > **PSIRT and EOX**.

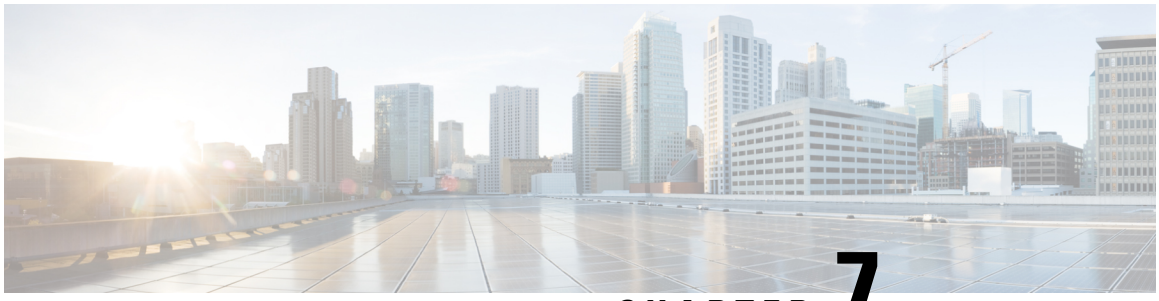
Step 2 Click **Schedule Job**. The **Schedule** dialog box appears. You can set the **Start Time** and **Recurrence** options and then click the **Submit** button to schedule the job. Click the **OK** button, in the pop-up that appears, to delete the already scheduled job and create a new one.

A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, Module Hardware EOX and Field Notice information is gathered and reported. You do not create separate jobs on each of the tabs.

Step 3 Click the **Field Notice** tab to view field notice information.

Step 4 Click on the *i* icon in the Vulnerable column to open the Field Notice URL and Caveat Details dialog box. Click on the Field Notice URL to view more information on cisco.com.

Step 5 (Optional) You can export the device field notice details in PDF and CSV format for each device and for all devices collectively.



CHAPTER 7

User-Defined Inventory Discovery Job

User-Defined Inventory Discovery Job

The Switch Inventory job is a system job that runs everyday to collect physical and logical inventory information of devices on the network. By default, this job runs for all devices on the network. You cannot customize this job to collect inventory only for a select set of devices or a device group. Also, you cannot abort any long running instances of this job with ease.

You can create user-defined Inventory Discovery jobs where you can:

- Collect inventory only for select set of devices or a device group.
- Customize the recurrence.
- Choose the number of times the job should run.
- Abort the job automatically when it's running for a longer time than expected.
- Choose to prioritize inventory collection on devices skipped from a previously aborted job run.

You can either run the default switch Inventory job or the user-defined Inventory Discovery job. You must disable the default switch inventory job before running any user-defined Inventory Discovery jobs. To do this:

1. Navigate to **Administration** > **Settings** > **System Settings** > **Inventory**.
2. Under **Inventory**, select the check box **Disable Switch Inventory Job** and click **Save**. Once you enable this setting, the default Switch Inventory job is disabled and the user-defined Inventory Discovery job is enabled.

To switch back to the default Switch Inventory job, clear the **Disable Switch Inventory Job** check box. This disables and suspends any scheduled user-defined Inventory Discovery jobs.

Note When you switch between the Inventory Discovery job and the Switch Inventory job (from Inventory Discovery job to Switch Inventory job for example) the job that you switch to is only enabled but does not run automatically. You will need to manually resume the job run by selecting the job from the Jobs Dashboard (**Administration** > **Dashboards** > **Jobs dashboard**) and clicking **Resume series**.

Create a User-Defined Inventory Discovery Job

To create a user-defined switch inventory job:

Before you begin

Disable the default Switch Inventory job. Navigate to **Administration** > **Settings** > **System Settings** > **Inventory**. Under **Inventory**, select the check box **Disable Switch Inventory Job** and click **Save**.

Note You can still create user-defined Inventory Discovery jobs even if you haven't disabled the default Switch Inventory job. These newly-created jobs remain suspended; you will be able to run these jobs after you disable the default Switch Inventory job.

Step 1 Navigate to **Administration** > **Dashboards** > **Jobs Dashboard** > **User Jobs** and click '**+**'.

Step 2 Specify a Job name. Alphabets, numbers, underscore, hyphen, and space are allowed. Special characters are not permitted.

Step 3 Click the **Select** toggle button to choose either by **By Device** or **By Group**.

- **By Device** - lists all the devices in the system. There is no limit on the number of devices you can choose.
- **By Group** - lists all system and user-defined groups. You can choose only one device group at a time.

Choose devices or a device group as necessary and click **Next**.

Step 4 Schedule the job by configuring the following settings:

Schedule Settings

- **Start time**: Specify the start date and time.
- **Recurrence**: Choose either **Hourly**, **Daily**, **Weekly**, **Monthly** or **Yearly**. The minimum recurrence time you can schedule is every 6 hours. This is also the default recurrence time.
- **End time**: Choose one of the options to specify an end time for the job.
  - **No End Date/Time** - if you do not wish to specify an end time and would like to run the job indefinitely.
  - **After** - to end the job after running the specified number of times. This option is available only if you choose **Recurrence** as **Hourly** or **Daily**.
  - **End at** - to end the job on a specific date and time.

Abort Settings

- **Abort Long running Job** - Select this check box and specify the cut-off time in hours and minutes. Any job running beyond the time you specify here will be aborted automatically. The minimum time you can specify is 2 hours.
- **Collect Abort Devices First in Next Run** - Select this check box to prioritize sync on aborted devices in the next run.

Step 5 Click **Finish**.

You can view the newly created job on the Jobs dashboard (**Administration** > **Dashboards** > **Jobs dashboard** > **User jobs** > **Inventory Discovery Jobs**). Select the job and click **Run** if you would like to run the job immediately. See Manage Jobs Using the Jobs Dashboard, on page 23 for more information.

Edit a User-Defined Inventory Discovery Job

Step 1 Select the Inventory Discovery job from the Jobs dashboard.

Step 2 Click **Edit Schedule** to modify the schedule settings.

Note You can only edit the schedule or abort settings. You cannot modify the devices or device group you chose when you created the job.

View Results on Jobs Dashboard

You can view the result of the job run on the Job dashboard.

Step 1 Navigate to **Administration** > **Dashboards** > **Jobs dashboard** > **User jobs** > **Inventory Discovery Jobs**.

Step 2 Click the hyperlink of the job.

The **Job Results** page for the job displays the following details:

- Collection summary of individual devices - Device Name, IP address, Start Time, End Time, Result
- Device-specific results to indicate:
  - Success - when inventory collection status on the device is Completed.
  - Failed - when inventory collection status on the device is Completed with Warning, Collection Failure or credential failure.
  - Cancelled - if the job was aborted.

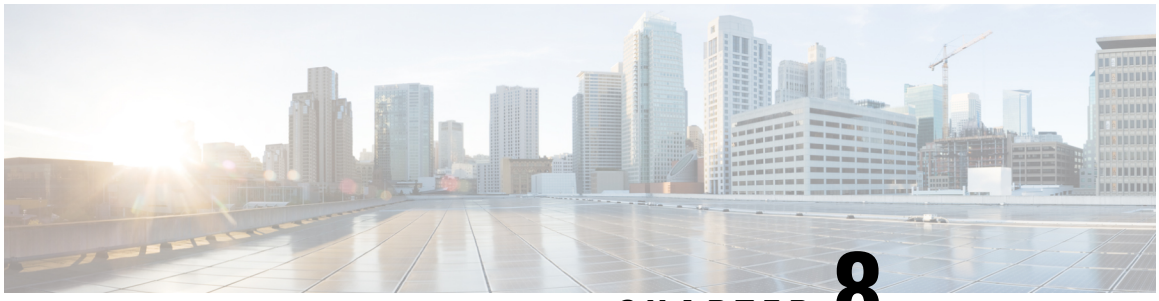
Note Devices that are not in Managed-Complete state will be skipped during the job execution. If any of the participating devices are already in sync, then those devices are skipped during the inventory discovery job execution and marked as Cancelled.

- Overall Job collection status as:
  - Success - if inventory collection was successful on all devices.
  - Failure - if inventory collection failed on all devices

- Partial Success - if inventory collection failed on some of the devices.
- Cancelled - if the job was aborted.

PART III

Visualize the Network



CHAPTER 8

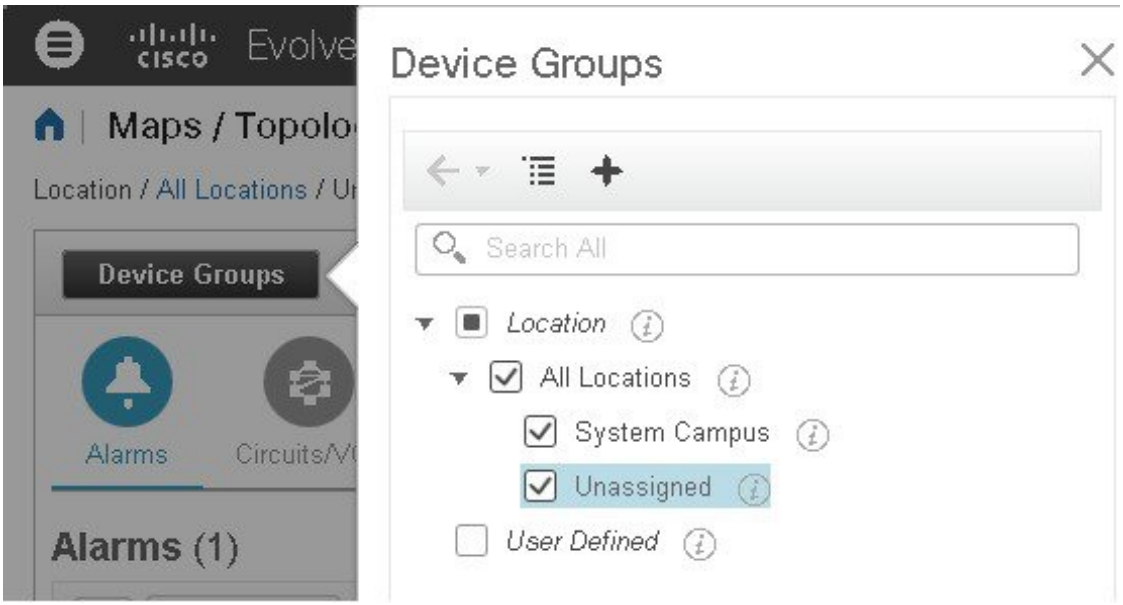
Visualize the Network Topology

This chapter provides the following topics:

Network Topology Overview

The Network Topology window presents a graphical, topological map view of devices, the links between them, and the active alarms on elements in the map. It also enables you to visualize circuits/VCs within the displayed topology map. In addition, the Network Topology window provides access to map element tools and functions, and allows you to drill-down to get detailed information about map elements.

The Network Topology window is accessed from the left sidebar (**Maps** > **Topology Maps** > **Network Topology**). The content of the Network Topology window is determined by the device group(s) you have selected. To select a device group, click the Device Groups button in the toolbar and select one or more groups in the Device Groups panel. From the Device Groups panel you can access the central device grouping functionality to create new groups, add devices to groups, and so on. See Create Groups of Devices for Easier Management and Configuration, on page 72 for more information.



Each Network Topology map is divided into a left pane that contains alarms/circuits/VCs/links information, and a right pane that displays the map itself. From the left pane, use the toolbar to control the spacing of both panes. For example, if you select 100%, only the map will be shown. If you select 50%, the map and the left pane will share the screen equally. When the left pane is expanded, additional columns might be added to the tables in the tabs.

- Alarms, Circuits/VCs, and Links (left pane)— Provides information relevant to the devices and topology shown in the map.
  - Alarms tab—Shows a table listing the current alarms for the selected group(s) and their severity. You can select alarms and perform basic actions, such as clear, acknowledge, and so on. For full details of the alarms, click the Alarms Table link at the bottom of the Alarms tab.
  - Circuits/VCs tab—Lists the circuits/VCs relevant to the devices in the selected group(s), and indicates the primary state of each circuit/VC. The primary state reflects the most serious current state of the circuit, as derived from the provisioning, serviceability, discovery, and alarm states. See Circuit or VC States, on page 620 . By default, the circuits/VCs are sorted by primary state, from most to least severe. Note that:
    - Selecting a circuit/VC in the list displays a visual representation of the circuit/VC in the topology map.
    - Clicking the Circuits/VCs link at the bottom of the tab launches a separate window with a table of circuits/VCs providing more details for each circuit/VC.
    - Clicking the Network Interfaces link at the bottom of the tab launches a table listing the interfaces that have been configured for participation in circuits/VCs, such as UNIs and ENNIs.
    - Clicking the appropriate toolbar icon allows you to perform actions such as creating a new circuit or running an ITU-T Y.1564 test on the selected circuit.
  - Links tab—Lists the links relevant to the selected device group(s) and shows the highest severity alarm on the link. Selecting a link in the table highlights the link in the topology map. Clicking the Links Table link at the bottom of the tab launches a separate window with a table of links.

- Topology map (right pane)—Displays the topology of the selected device group(s) in graphical form. It displays the group's devices and sub-groups (if any) and the links between them (Physical, Ethernet, and technology-specific links). It also displays the active alarms on the devices or links so that you can easily identify problems in the network. You can drill down from the topology map to detailed information about a device or link in order to troubleshoot problems. The topology map can be customized, filtered, and manipulated to show exactly the information you need.

  You can toggle between the network topology map and the geographical map using the toggle buttons in the top right corner of the map.

  Use the **Auto-Refresh** drop-down list at the top-right corner of this pane to select the refresh time interval at which Alarms, Circuits/VCs, and Links table in the topology map view are refreshed. You can set the refresh interval to **Per user preferences** (see Change User Preferences, on page 25 for more information), **Every 10 seconds**, **Every 30 seconds**, or **No auto-refresh**.

Note If you choose **Every 10 seconds**, by design the Alarms tables in the Topology map do not display the **Actions** option.

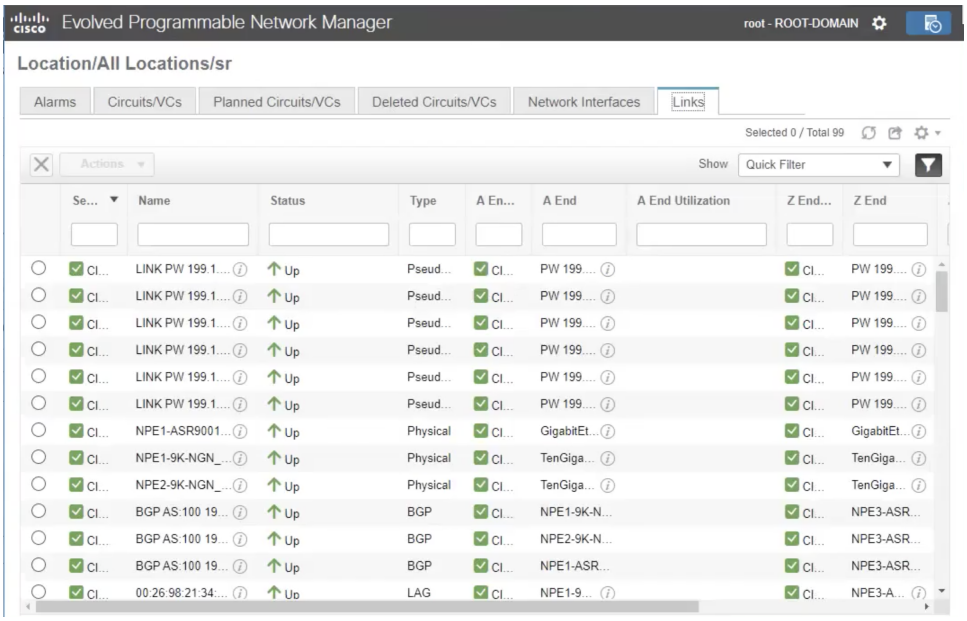
View Detailed Tables of Alarms, Network Interfaces, Circuits/VCs, and Links from a Network Topology Map

From the Network Topology window, you can access extended tables that list and provide more information about the alarms, network interfaces, circuits/VCs and links in the selected device group. These extended tables open in a separate browser window.

The tables accessed from the Network Topology window contain information for the selected device group only. You can access a full list of all alarms/circuits/planned circuits/deleted circuits/network interfaces/links in the system by selecting **Inventory** > **Other** and then selecting the required table (links, network interfaces, and so on).

To open the extended details tables, click the **Detach** icon in the top right corner of the tab or click on the hyperlink at the bottom of a specific tab, for example, click on the Alarms Table link at the bottom of the Alarms tab.

The window displaying the extended tables has these tabs: Alarms, Circuits/VCs, Planned Circuits/VCs, Deleted Circuits/VCs, Network Interfaces, and Links.



Be aware of the following when working with the extended tables:

- When the extended tables window is open, the left pane of the Network Topology window is disabled. When you close the extended tables window, the tabs in the left pane of the Network Topology window become fully functional again.
- There is synchronization between the extended tables and the corresponding tabs in the Network Topology window. For example, if you select a circuit/VC in the extended Circuits/VCs table, that circuit will also be selected in the Circuits/VCs tab in the Network Topology window and the circuit/VC overlay will be shown in the topology map. Conversely, if you select a circuit/VC in the Network Topology window and then open the extended table, the same circuit/VC will be selected in the extended table.
- All the tables in the Network Topology view are refreshed based on the setting you choose in **Auto-Refresh** drop-down list in the upper right corner of the page. You can set the refresh interval to **Per user preferences** (see Change User Preferences, on page 25 for more information), **Every 10 seconds**, **Every 30 seconds** or **No auto-refresh**. The default refresh interval is **Per user preferences**.

Note If you choose the **Every 10 seconds**, by design the tables in the Topology view will not have the **Actions** option.

- Click the **Export** icon at the top right of the table to export the data from the table to a file.

Note Only CSV format is supported for Circuits/VCs and Network Interface tables. The data from these two tables is exported irrespective of any filters or UI page. For the other tables, **Export** supports both CSV and PDF formats and data is exported based on the applied filters and the current UI page.

- Click the *i* icon next to the **Provisioning** column in the Circuits/VCs and Deleted Circuits/VCs tabs to view the details of configuration, configuration errors, rollback configuration, and rollback configuration errors for each device participating in the circuit/VC. The *i* icon is available for all provisioning states, except None.

Filter Data in the Detailed Tables

You can also filter the data to find specific alarms, circuits/VCs, network interfaces, or links using a *quick filter* or an *advanced filter* from the **Show** drop-down list. The quick filter narrows the content that is displayed in a column according to the text you enter above the column. The advanced filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. You can also create a *user defined* filter which, if saved, will be added to the **Show** drop-down menu.

To create and save a user defined filter:

Step 1 From the **Show** drop-down list above the extended tables of alarms, circuits/VCs, network interfaces, and links, choose **Advanced Filter**.

Step 2 In the **Advanced Filter** data popup window, enter the advanced filter criteria, and then click **Save As**.

Step 3 In the **Save Filter** dialog box, enter a name for your filter and click **Save**.

To edit or remove a user defined filter, choose **Manage User Defined Filters** from the **Show** drop-down list.

Search for a Device in the Map

You can search for devices in the topology map and in the geo map by the following criteria:

- Device name
- Device family
- IP address
- User defined field value

To search for specific devices in the map:

Step 1 Click the **Search** icon in the toolbar.

Step 2 Type the full or partial device name/IP address/device family/user defined field value in the search text box and press **Enter**. In the topology map, you will see a list of devices that match the search criteria. In the geo map, the Search Results panel lists the devices that match your search and indicates whether they are mapped or unmapped. Click on the i icon to show the Device 360 which contains more information about the device. Click on a device to highlight it in the map.

Determine What is Displayed in the Topology Map

Choose Which Device Group(s) to Display in the Network Topology Map

The topology map enables you to visualize the topology of a device group or multiple device groups. The selected group(s) might cover a specific network segment, a customer network, or any other combination of network elements. Device grouping is hierarchical. There are two top-level parent groups containing multiple sub-groups - Location groups and User Defined groups. You can display multiple groups within the same top-level parent group. For example, you can display multiple Location groups but you cannot display one Location group and one User Defined group.

To determine which devices are displayed in the topology map, click on the **Device Groups** button in the left pane and select one or more device groups.

The maximum number of devices that can be displayed per group on the topology map is 1500. When you load the topology map, Cisco EPN Manager displays the following warning messages at two thresholds:

- 1000 devices – displays the map with a popup message to indicate possible slowness
- 1500 devices – displays an empty map with a popup message to indicate that the map cannot be displayed for so many devices

Note The threshold limits are based on the number of devices and not on the number of links between the devices.

After you have displayed the required group(s) in the topology map, you can access additional information about any device or link. See Get More Information About Devices, on page 185 and Get More Information About Links, on page 186.

The topology map only displays devices for which the logged in user has access privileges, based on the virtual domains to which the user has been assigned.

Note If you encounter topology issues, such as topology components not rendering as expected or component data not being displaying on the map, we recommend that you clear your browser cache and try again.

To display network elements in the topology map:

Step 1 Choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click on the **Device Groups** button in the left pane to open the Device Groups panel.

Step 3 Click on the device group(s) you want to display in the topology map and click **Load**. The device group selections are displayed above the topology map.

Step 4 Customize the topology map as required by showing specific device/link types, adding manual links, and so on. See the following topics for more information:

- Change Which Link and Device Types are Shown in the Network Topology Map, on page 182
- Manually Add Links to the Topology Map, on page 180
- Change the Layout of a Network Topology Map, on page 194

View the Contents of a Sub-Group in the Topology Map

You can expand a sub-group to show its contents within the current context or you can drill down to see the contents of the sub-group independently of the current map context.

Note When expanding sub-groups, be aware that if a device belongs to more than one group, the device will appear in one of the expanded groups only. It will not appear in all of the groups to which it belongs. If your setup has devices that belong to multiple groups, rather view the groups individually in the topology map by selecting them in the Device Groups pane. This will ensure that you will always see all the devices that belong to a specific group.

To view the contents of a sub-group:

Step 1 Click on a sub-group in the topology map.

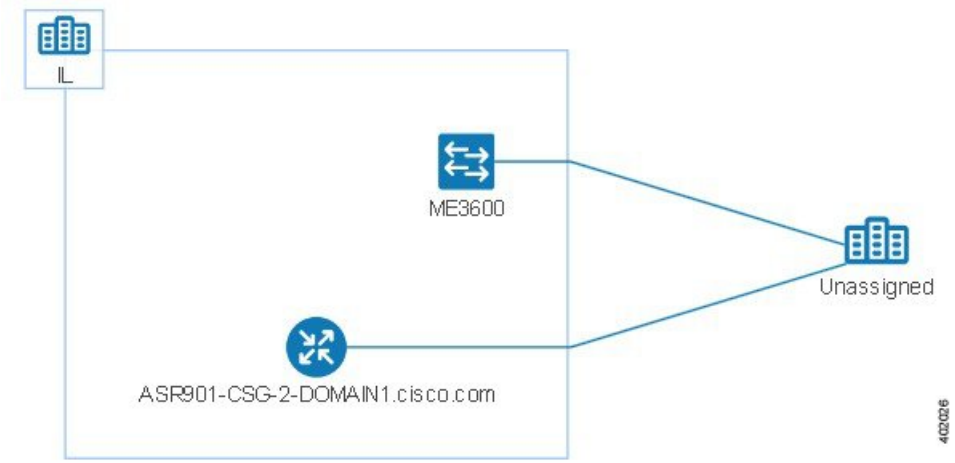
Step 2 In the displayed popup, click one of the following:

- Drill down group—Displays the sub-group on its own in the topology map, meaning that the currently displayed group is replaced with the selected sub-group. Note that the sub-group name is selected in the Device Groups pane.

  Note You can double-click on the sub-group to quickly drill down into the group.

- Expand group—Adds the contents of the sub-group to the current topology map display.

In the figure below, the IL group is expanded.



Manually Add Devices and Networks to the Topology Map

You can display devices and networks that are not managed by the system on the topology map and on the geo map by adding them manually.

Step 1 In the topology toolbar, choose **Create > Create Unmanaged Device** or **Create > Create Unmanaged Network**.

Step 2 Click on the map to add the device/network to the map.

Step 3 Click on the newly-added device/network in the map. From the displayed panel, you can add the device/network to a group, rename the device/network, or delete the device/network.

After you have added a device or network to the topology map, it will also be available in the geo map. The unmanaged device will appear in the list of unmapped devices and you can set its location. See Place Unmapped Devices on the Geo Map, on page 206.

Manually Add Links to the Topology Map

If you know that two devices are connected but Cisco Evolved Programmable Network Manager cannot discover the link and show it on the map, you can add the link manually. After you add this link, it will be shown by default whenever the relevant group is shown on the map.

Following are the most common scenarios in which manual links could be used:

- From the optical/DWDM controller of a trunk port on a Cisco NCS device running IOS-XR (NCS 4000, 9000, 5000, 1000) to an add/drop port pair in NCS 2000 devices.
- From the optical/DWDM controller of a client port on a Cisco NCS device running IOS-XR (NCS 4000, 9000, 5000, 1000) to NCS 2000 transponder client ports (representing connections for 10GE/100GE ports).
- From 10GE/100GE controllers of ports on a Cisco NCS device running IOS-XR (NCS 4000, 9000, 5000,1000) to NCS 2000 transponder client ports (representing connections for 10GE/100GE ports).

- Between two trunk ports on Cisco NCS 2000 series devices with 400-G-XP linecards. This link must be created as a managed OTU link.
- From a Cisco NCS 2000 series device with 400-G-XP linecard and a Cisco NCS 4000 series device with 4H-OPW-QC2 linecards. This link must be created as a managed OTU link.

Manual links can be managed or unmanaged :

- Unmanaged links: For visualization purposes only. If you know that two devices are connected but you do not need full management of the link between them, you can add an unmanaged manual link to the map. The link will appear as a grey dashed line.
- Managed links: When you add a managed manual link, it is saved to the database and is included in all links tables. It is shown on the map as a solid line, the same as all other managed links. Cisco EPN Manager retrieves the link status from the managed device interfaces to which it is connected. The discovery status of a manually added managed link will be "Pre-provisioned." This indicates that it was not discovered by the system.

Note If you accidentally delete one device, delete the other end of the managed link too before you recreate the managed link.

To manually add a link between two devices:

Step 1 In the topology toolbar, choose **Create** > **Create Unmanaged Link** or **Create** > **Create Managed Link**.

Step 2 Click and hold down the mouse on the first device in the topology map and drag it to the second device.

Step 3 In the Interface Details dialog, select the source interface on the first device and the target interface on the second device from the drop-down lists of available interfaces, and click **OK**.

Note Make sure that the endpoints are not part of another link. For IOS-XR devices to SVO Add/Drop ports, two managed links have to be created to form an aggregated link.

The link between the two selected devices will be displayed on the map.

Delete a Manually Added Link

Links that were added manually to the map can be deleted from the system.

- Manually added managed links are deleted from the Links table, as described in the procedure below.
- Manually added unmanaged links are deleted by clicking on the link in the map and then clicking **Delete** in the Link panel.
- Make sure you delete the managed link before you delete the endpoints.
- In the SVO nodes, do not delete the cross connections before deleting the managed links.

To delete a manually added managed link:

Step 1 In the left sidebar, choose **Inventory** > **Other** > **Links**.

Step 2 Filter the Status column of the Links table to show Pre-provisioned links and select the required link.

Step 3 Click the Delete icon to delete the link. The Delete icon is only enabled for manually added links.

Step 4 Alternatively, to delete the manually created links, click the information (I) icon on the link that you want to delete.
In the **Link Details** window, a single link with **Type** as "Manual" appears.

Step 5 Choose the entry and then click the Delete (X) icon to delete the link.

To delete a manually added unmanaged link:

a. Filter the Status column of the Links table to show Pre-provisioned links and select the required link.

b. To delete the manually created unmanaged links, click the information (I) icon on the link that you want to delete. In the **Link Details** window, a single link with **Type** as "Manual" appears.

c. Choose the entry and then click the Delete (X) icon to delete the link.

Rename a Link

By default, the link name is generated automatically by the system based on the A- and Z-end interface name. You can rename any link, in which case the new name will represent the link in all link tables, in the Link 360 view, and on the map.

To rename a link:

Step 1 Go to any of the link tables.

Step 2 Select the link you want to rename.

Step 3 Choose **Actions** > **Rename**.

Step 4 Enter a unique name for the link and click **Rename**.

Change Which Link and Device Types are Shown in the Network Topology Map

You can choose to display only certain types of links or devices in the network topology map. Click the **Show** button and select **Links** or **Device Families** to see a full list of link and device types and select the ones you want to display.

Note Link/device type filters are disabled when you select a specific circuit/VC to display on the map.

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click on the **Device Groups** button, select the required device group(s), and click **Load**.

Step 3 Click **Show** in the topology toolbar and choose **Links** or **Device Families**.

Step 4 In the Links dialog:

- Select the types of links you want displayed in the topology map, for example, physical layer links, Ethernet layer links, and so on. The Links dialog only shows link types that exist in your network. If a link type exists in your network but not in the selected device group, it will be disabled.
- If you want to differentiate aggregated links from single links, select the Display Aggregated Links as check box.
- You can enable bandwidth utilization visualization on links that support this feature. See Show Bandwidth Utilization for Links on the Map, on page 192 for more information.
- Click **OK**. The topology map will reflect your selections. Only the link types you selected will be displayed.

Step 5 In the Devices dialog:

- Select the device types you want displayed in the topology map, for example, routers, switches and hubs, optical networking, and so on. The Devices dialog only shows device types that exist in your network. If a device type exists in your network but not in the selected device group, it will be disabled.
- Click **OK**. The topology map will reflect your selections. Only the device types you selected will be displayed.

Note If you have selected to display optical networks on the map, by default you will see the devices that serve as optical line amplifiers (if any). Deselect the Display Optical Line Amplifier check box under Device Functions if you do not want these optical line amplifier devices to be displayed on the map. The Display Optical Line Amplifier check box under Device Functions only appears if there are optical devices in setup which support Line Amplifier functionality.

Show/Hide Labels in the Topology Map

You can choose to hide the device name labels.

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Show** button in the topology toolbar.

Step 3 Select the **Labels** check box.

Step 4 Close the Show dialog. Your selections are applied to the topology map.

Filter Devices and Links by Alarms

To view only the devices or links containing alarms and suppress the rest of the devices:

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Show** in the topology toolbar and select **Alarms**.

Step 3 Select the check box to show all alarms or use the slider to show alarms of a certain severity or higher.

Step 4 Select **Show only elements with the selected alarms** to view only the devices and links containing alarms.

Step 5 To save and close the Show dialog, click **OK**.

Save Global Preferences for the Map Display

The **Show** button in the map toolbar allows you to choose the items that will be shown in your map display, including device names (labels), device types, link types, alarm severity, and so on.

If you are a Super User or Admin user, you can save your choices as global preferences which will be applied automatically for all new users and which can be loaded by any users on demand. You can also delete global preferences.

Note Any user having Network Topology Edit permission, will be able to save and delete the global preference. You also need to have the Network Topology permission to access the topology maps.

The following items are saved as global preferences:

- Labels on/off
- Device families
- Link types
- Alarm severity
- Bandwidth utilization

To save global preferences for map display:

Step 1 In the left sidebar, choose **Maps > Topology Maps > Network Topology**.

Step 2 Click on the **Device Groups** button, select the required device group(s) and click **Load**.

Step 3 Click **Show** in the topology toolbar and select the items you want to show on the map.

Step 4 Choose **Global Preferences > Save**.

Saved global preferences can be deleted if necessary by clicking **Delete**.

Load Global Preferences for the Map Display

The **Show** button in the map toolbar allows you to choose the items that will be shown in your map display, including device names (labels), device types, link types, alarm severity, and so on.

If global preferences have been defined for the map display, you can load them. You can then make your own changes to the map display as required.

The following items are saved as global preferences:

- Labels on/off
- Device families
- Link types
- Fault severity
- Bandwidth utilization

To load global preferences for map display:

Step 1 In the left sidebar, choose **Maps > Topology Maps > Network Topology**.

Step 2 Click on the **Device Groups** button, select the required device group(s) and click **Load**.

Step 3 Choose **Global Preferences > Load**. This option is disabled if no global preferences have been defined.

Isolate Specific Sections of a Large Topology Map

In cases where a topology map is displaying thousands of devices, you might want to focus on specific devices or sets of devices. The Overview pane shows you the entire topology map in miniature and lets you select the area you want to display in the large topology map. It also provides an at-a-glance view of the alarm status of the elements in the topology map.

Step 1 Click the Overview icon in the topology toolbar. The Overview pane appears in the at the bottom right of the topology map and displays the following:

- Dot—indicates any network element. The color of the dot indicates the severity of alarms associated with the network element.
- Line—indicates a link. The color of the line indicates the severity of the associated alarm.
- Blue rectangle—indicates the selection area. The area within the rectangle is displayed in the map pane. Handles on the corners enable you to resize the selection area.
- Pan mode cursor—cursor displayed within the selection area. Use this cursor to move the selection area, and thereby view different elements in the map pane.
- Zoom mode cursor—displayed outside the selection area. Use this cursor to define a new selection area or to zoom in on an existing selection area.

Step 2 Draw a rectangle by dragging the mouse over the area you want to see in the topology map.

Step 3 Click the ‘x’ in the upper right corner to close the Overview pane.

Get More Information About Devices

From the topology map, you can drill down to get more information about a device.

Step 1 Click on the required device in the topology map. A popup appears showing basic device information and alarm information for the device.

Step 2 Click **View 360** to access the Device 360 view for detailed information about the device.

For more information, see, Get Basic Device Information: Device 360 View, on page 84.

Get More Information About Links

Cisco EPN Manager provides a variety of ways that you can view links and get more details about them:

To view link information for:	See the procedures in:
A specific link	Get a Quick Look at a Specific Link: Link 360 View, on page 186
A specific link in a topology map	View a Specific Link in the Topology Map, on page 189
A group in a topology map	View a Device Group's Links in a Network Topology Map, on page 189
All of Cisco EPN Manager	View Link Tables , on page 190

Get a Quick Look at a Specific Link: Link 360 View

The Link 360 view gives you a quick look at the configuration and status of a device's links. Each Link 360 view provides information about the A- and Z-sides of the link (type, direction, capacity, and so forth). Depending on the link and device type, it also provides a wide range of metrics, such as power level, span loss, and bit errors.

You can launch the Link 360 view by clicking the "i" next to a link name in any of the link tables. This includes the tables that are opened by clicking **Links Table** in a topology map, or by choosing **Inventory** > **Other** > **Links**.

The Link 360 view provides general link and performance information at the top of the view, and more detailed link information in tabs in the lower part of the view.

Information Provided in Link 360 View	Description

General information	The link name, serviceability status, highest severity alarm, type, direction, capacity, and utilization. Definitions of link serviceability states are provided in Link Serviceability States, on page 187. If the link you are viewing is an OTS or OTU link, you can click the **Utilization** field's *i* (**information**) icon to open the **Used Wavelengths** pop-up window, which lists the optical channels configured on the link and the circuits that are currently using those channels. Auto-Refresh—For real-time updates of status and troubleshooting, enable an on-demand refresh by clicking on the Refresh icon. Alternatively, you can also set the auto-refresh interval to 30 seconds, 1 minute, 2 minutes or 5 minutes from the drop-down list. Auto-Refresh is OFF by default. **Note** The Auto-Refresh setting is applicable only for the currently open 360 view popup window. If the view is closed and reopened or another view is opened, by default Auto-Refresh is Off.
Performance data	Graphs or charts reflecting various aspects of link performance.
Span Loss	Channel span loss data is displayed along with the minimum and maximum threshold and resolution. If the span loss data is out of range, it is displayed in red.
Alarms	Current alarms for the link, including their severity, status, the time they were generated, the source of the alarm, and the alarm's ID. Also provides a launch point for the Alarm Browser.
Links	(LAGs only) Status, name, and IP address for the A-side and Z-side port in the Link Aggregation Group.
Endpoints	Devices and interfaces that serve as endpoints for the link. Provides a launch point for the Interface 360 view. For optical devices, this tab also displays the latest recorded power values for transmitted and received signals. **Note** Power values are not normally displayed for manual links. However, if you open the Link 360 view for a manual LMP or OTS link between a Cisco NCS 1000 and 2000 device, the view displays the power values for both endpoints.
Circuit/VCs	(For a circuit/VC that traverses the link) Circuit/VC name, type, customer, status, and creation date. Also provides a launch point for the Circuit/VC 360 view.
SRRGs	Lists the Shared Risk Resource Groups (SRRGs) assigned to the link or to the link endpoint devices. For each listed SRRG, you can see whether it is the default SRRG on the link/device or if it has been assigned to the link/device. For more information about SRRGs, see Manage Shared Risk Resource Groups (SRRGs) in the Geo Map.
APC	Lists the sides, admin status, APC status, and progress status of the link.

Link Serviceability States

Serviceability State	Icon	Description

Admin Down		Link was purposefully shut down by the administrator.
Down		Link is down (but it should not be).
Up		Link is up and traffic is passing through the link.
Auto Up		Link is up because it detected a signal (this state is only supported by optical devices).
Unavailable		Link is not discovered yet or its status is unavailable.
Partial		Link has a mismatch between requests, resources, or resource states. Examples: • Link is processing a request to activate some service resources and deactivate others. • Link has some active and some deactivated resources. • Some link resources are up and others are down. • The state for one of the link's resources is not known.

Compare Link Information and Status

From the **Comparison View**, you can perform a side-by-side comparison of multiple links, viewing information such as raised alarms and the status of associated endpoints, circuits, and VCs. To compare links, do the following:

Step 1 For each link you want to compare:

a) Open its **Link 360** view, as described in Get a Quick Look at a Specific Link: Link 360 View.

b) Choose **Actions** > **Add to Compare**.

The link you selected is displayed at the bottom of the page. You can select a maximum of 4 links.

Step 2 Click **Compare**.

The **Comparison View** opens.

Step 3 From the drop-down list at the top of the view, specify whether the view will show all available information or just the information that is unique to each link.

Step 4 Click **Comparison View**, check the check box for the categories you want the view to display, and then click **Save**.

By default, all of the categories are already selected.

Step 5 Scroll down the page to view the information provided for each category you selected.

Note the following:

- The **Comparison View** only displays information for two links at a time. If you selected more than two, you will need to toggle to the links that are not currently displayed.
- To reorder the links you have selected, click **Rearrange**.

- Each link's **Actions** menu is identical to the one provided in its **Link 360** view. If you select an option, the corresponding page opens.
- You can minimize and maximize the categories displayed, as needed.
- The **Comparison View** is also available for circuits and VCs, devices, and interfaces. Whenever you select any of these elements from their respective 360 view for comparison, they are displayed in the corresponding tab. This allows you to switch between element types, as needed.
- When you are done comparing links, click **Back** at the top of the view and then click **Clear All** at bottom of the page. If tabs for other element types are still displayed, you will need to clear them as well.

View a Specific Link in the Topology Map

You can select a specific link from the following pages and view the link in the topology map:

- Launch the Link 360 view, and then choose **Actions** > **Show in Topology**. For information about how to launch the Link 360 view, see Get a Quick Look at a Specific Link: Link 360 View, on page 186.
- From the links table, select a specific link, and then choose **Actions** > **Show in Topology**. You can access the links table by clicking the Links Table hyperlink under the Links tab in the topology map, or by choosing **Inventory** > **Other** > **Links**.

View a Device Group's Links in a Network Topology Map

Cisco EPN Manager uses the following conventions to represent links in the topology map:

- A solid line represents any type of discovered link between two elements in the topology map.
- A dotted line represents an unmanaged link that was manually drawn in the topology.
- (If enabled in the **Show > Links** menu) A dot-dash line represents an aggregated link.
- If there is a critical alarm on a link, the link will be colored red and the alarm icon will be displayed on the link.
- If an existing link is down and there is no critical alarm on the link, the link will be colored grey and a "?" icon will be displayed on the link. After 6 hours, the link will be removed automatically from the map but it can be deleted manually from the Links table or from the Link details view before that time if necessary.

If an alarm severity badge is displayed on a link, it represents the most severe alarm that is affecting the link. For aggregated links, it represents the most severe alarm affecting any of the links in the aggregation.

To get more information about links in a topology map:

- Hover over the link with your mouse to display a panel that provides "at-a-glance" useful information about that link, such as the most severe alarms, or bandwidth utilization information for the link, if available. If there are no alarms on the link and there is no bandwidth utilization information, this panel will not be displayed. If there are alarms on the link, you can click the number next to the alarm severity icon to display a table listing only those alarms.

- Click on a link to display a popup window with link information, including link type, the link's A- and Z-side devices and interfaces, and link utilization. For aggregated links, the popup window lists all the underlying links. If the number of links exceeds 200 links in a single line, Cisco EPN Manager displays a warning message in the links panel and displays only 200 links.

View Link Tables

Cisco EPN Manager provides a table that lists all of the links that it is managing. This provides a quick way to locate all links of a specific type or with a name that shares a common string. You can also identify links that have severe alarms, and launch Interface 360 views for view the affected sides.

The table also provides a quick look at link utilization and capacity.

In addition, you can open a table showing links for the current group being displayed in the topology map. This table provides the same information and actions as the table of all links in the system.

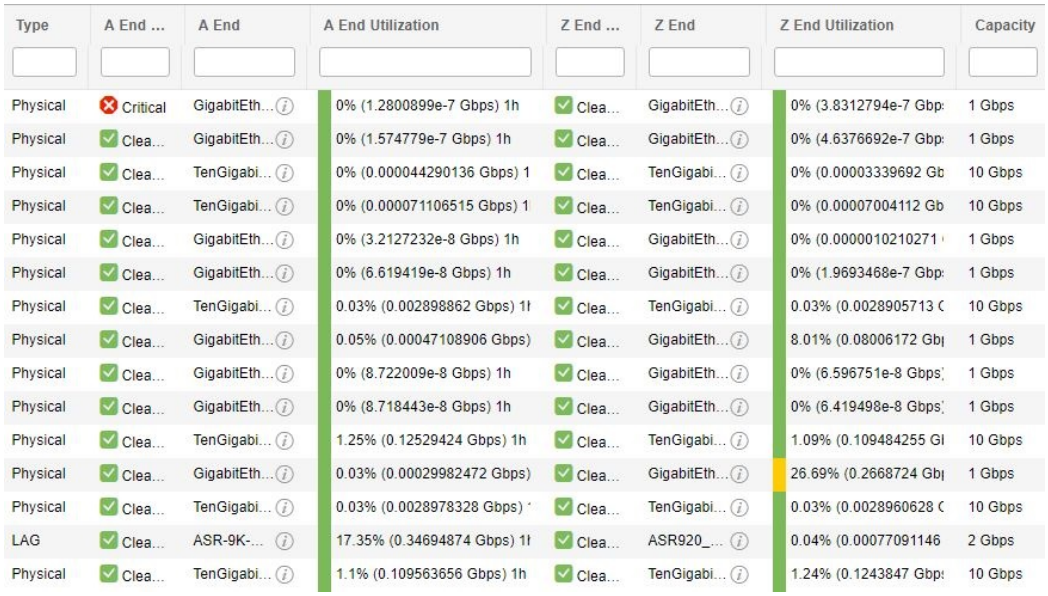
Step 1 To display link tables:

- For all links: In the left sidebar, choose **Inventory** > **Other** > **Links**.
- For a selected device group's links: In the left pane of the topology map window, select the Links tab, then click the **Detach** icon in the top right corner or click the Links Table hyperlink at the bottom of the tab. The Links table is displayed in a separate window.

Step 2 From here you can do the following:

- Find specific types of links—for example, Physical, LAG, ODU, and so forth. Place your mouse cursor in the Type field and select the link type from the drop-down list. You can also find Manual Links in this manner.
- Find links by name by entering text in the Link Name text box. You can also enter a partial string (for example, **3.3.3.3_**).
- Find links with severe alarms by clicking in the Severity text box to display a severity drop-down list, then choosing a severity. You can perform this same procedure from the A-side or Z-side. The table indicates which side of the link has the more severe alarm, and you can launch an Interface 360 view for both sides.
- See the operational and discovery status of links in the Status column. Links can have an operational status of Up or Down. The discovery status can be one of the following:
  - Preprovisioned: Managed links that were created manually by a user and were not discovered by the system. These links can be deleted from the system and from the map. Select the link and click the Delete icon.
  - Pre-provisioned-Incomplete: Manually created links that could not be fully discovered.
  - Discovered-Incomplete: Links that could not be fully discovered. These partially discovered links are not shown on the topology map.
  - Unknown: Existing links that are down and therefore can no longer be discovered. These links remain on the topology map for 6 hours but they are colored gray and are identified by an "?" icon on the link. Links with Unknown status can be deleted by selecting the link in the table and clicking the **Delete** button.
- See bandwidth utilization for optical (OTS, OTN, ODU) and packet (physical, LAG) links. The Utilization column for each side of the link shows the actual usage data (for example, number of channels for OTS links), the percentage of total capacity used, and the default time period for which utilization is calculated (1 hour). The Capacity column shows the total bandwidth capacity of the link.

Note To show utilization for packet and cable links, an Interface Health monitoring policy must be created and enabled on the relevant devices. See Set Up Basic Interface Monitoring, on page 225 for more information.



Type	A End ...	A End	A End Utilization	Z End ...	Z End	Z End Utilization	Capacity
Physical	Critical	GigabitEth...	0% (1.2800899e-7 Gbps) 1h	Clea...	GigabitEth...	0% (3.8312794e-7 Gbp:	1 Gbps
Physical	Clea...	GigabitEth...	0% (1.574779e-7 Gbps) 1h	Clea...	GigabitEth...	0% (4.6376692e-7 Gbp:	1 Gbps
Physical	Clea...	TenGigabi...	0% (0.000044290136 Gbps) 1	Clea...	TenGigabi...	0% (0.00003339692 Gb	10 Gbps
Physical	Clea...	TenGigabi...	0% (0.000071106515 Gbps) 1	Clea...	TenGigabi...	0% (0.00007004112 Gb	10 Gbps
Physical	Clea...	GigabitEth...	0% (3.2127232e-8 Gbps) 1h	Clea...	GigabitEth...	0% (0.0000010210271	1 Gbps
Physical	Clea...	GigabitEth...	0% (6.619419e-8 Gbps) 1h	Clea...	GigabitEth...	0% (1.9693468e-7 Gbp:	1 Gbps
Physical	Clea...	TenGigabi...	0.03% (0.002898862 Gbps) 1h	Clea...	TenGigabi...	0.03% (0.0028905713 (	10 Gbps
Physical	Clea...	GigabitEth...	0.05% (0.00047108906 Gbps)	Clea...	GigabitEth...	8.01% (0.08006172 Gbp	1 Gbps
Physical	Clea...	GigabitEth...	0% (8.722009e-8 Gbps) 1h	Clea...	GigabitEth...	0% (6.596751e-8 Gbps)	1 Gbps
Physical	Clea...	GigabitEth...	0% (8.718443e-8 Gbps) 1h	Clea...	GigabitEth...	0% (6.419498e-8 Gbps)	1 Gbps
Physical	Clea...	TenGigabi...	1.25% (0.12529424 Gbps) 1h	Clea...	TenGigabi...	1.09% (0.109484255 Gl	10 Gbps
Physical	Clea...	GigabitEth...	0.03% (0.00029982472 Gbps)	Clea...	GigabitEth...	26.69% (0.2668724 Gbp	1 Gbps
Physical	Clea...	TenGigabi...	0.03% (0.0028978328 Gbps)	Clea...	TenGigabi...	0.03% (0.0028960628 (	10 Gbps
LAG	Clea...	ASR-9K-...	17.35% (0.34694874 Gbps) 1h	Clea...	ASR920_...	0.04% (0.00077091146	2 Gbps
Physical	Clea...	TenGigabi...	1.1% (0.109563656 Gbps) 1h	Clea...	TenGigabi...	1.24% (0.1243847 Gbps	10 Gbps

- Depending on the link type, perform an action by choosing a link and making a selection from the **Actions** drop-down menu. (For example, for OTS links, you can run an OTDR Scan).
- View a specific link on the topology map by clicking **Actions** > **Network Topology**.

Troubleshoot Link Issues

This section presents suggested solutions for issues you might encounter when working with links.

Link Issue	Possible Cause	Solution
Links that previously existed disappear from the topology map.	The hostname might have been changed on one of the endpoint devices.	1. Delete the device on which the hostname was changed from the system and then add it again. 2. Sync the device and all devices connected to it to make sure that all information is updated.

Show Bandwidth Utilization for Links on the Map

In the topology map and in the geo map, you can enable visualization of how much bandwidth is utilized on optical links (OTS, OTN, and ODU), packet links (physical and LAG), and cable links (L2TP) over which circuits are provisioned. In this way, you can easily identify when a link is over-utilized or approaching over-utilization.

To enable bandwidth utilization, click on the arrow next to the **Bandwidth Utilization** icon in the top right corner of the topology map or the geo map and select the **Utilization** check box. For physical and LAG links, you can select the time frame in which to show the link utilization by clicking the arrow next to the Utilization check box. The MPLS links bandwidth utilization value in MPLS link 360 View is not available when WAE is not integrated.

When bandwidth utilization is enabled, a thicker link is shown in the map and is colored based on bandwidth utilization thresholds. Click the "?" icon in the Utilization panel at the top right of the map to see the color representations for bandwidth utilization on the supported link types. The thresholds for bandwidth utilization coloring can be set up in Administration > Settings > System Settings > Maps > Bandwidth Utilization. See Define Color Thresholds for Link Bandwidth Utilization, on page 193 .

Bandwidth utilization data is provided in all link-related views, for example, the Link panel that is displayed when you click on a link, Links tables, the Link 360, and so on, even if bandwidth utilization visualization is disabled.

Bandwidth utilization is calculated as follows:

- For OTS links between NCS 2000 devices, link capacity is calculated from the fiber-attributes parameters configurable on the devices. If OTS links are configured to allow SSON circuits (channel number is set to "Nyquist"), capacity is assumed to be 96 channels. Bandwidth utilization is calculated in terms of the number of 50Ghz ITU channels used in relation to the capacity. For SSON circuits the result is approximated because each Carrier NC or Carrier Trail counts as one channel used, regardless of its actual size.

  Click on the **i** icon in the Utilization column to display a dialog showing details of exactly which channels are being used and which circuits are using the channels.

Note The dialog shows only50 Ghz ITU wavelengths/frequencies, therefore SSON carrier circuits might not be shown.

- For OTN and ODU links, bandwidth utilization is calculated based on the number of ODU0 timeslots reserved and is represented in gigabits per second.
- For physical and LAG links, bandwidth utilization is calculated from the input and output data rate of the link interfaces. For these link types you can define whether you want to see the average utilization or the peak utilization. You can also specify the time period for which you want to show utilization data - 15 minutes, 1 hour, 6 hours, or 1 day.
- For cable L2TP links, L2TP utilization is calculated for available L2TP tunnels. If L2TP tunnels are present then L2TP link utilization is calculated per RPD by getting the OFDM channels utilization of the associated downstream controller.

Note To show utilization for packet and cable links, an Interface Health monitoring policy must be created and enabled on the relevant devices. See Set Up Basic Interface Monitoring, on page 225 for more information.

Define Color Thresholds for Link Bandwidth Utilization

When bandwidth utilization visualization is enabled, links in the map are colored based on the percentage of total bandwidth currently utilized on the link. See Show Bandwidth Utilization for Links on the Map, on page 192. Default thresholds are defined by the system, however, you can define your own thresholds to determine how bandwidth utilization will be reflected on the links.

To define color thresholds:

Step 1 Select **Administration > Settings > System Settings > Maps > Bandwidth Utilization**.

Step 2 Select the type of link for which you are defining thresholds.

Step 3 In the Link Coloring Thresholds area, define the criteria for coloring the links. Each row defines a color and the bandwidth percentage range that the color will represent. The default thresholds are: Green - 0-25%, Yellow - 26-50%, Orange - 51-75%, and Red - 76-100%.

Note the following:

- A maximum of 4 thresholds can be defined.
- The first threshold must start from zero and the last threshold must end with 100.
- The thresholds must be sequential, meaning that each row's range must follow on from the previous row's range. For example, if the range in row 1 is 0-25%, row 2's range must start with 26%.

Step 4 Click **Save**.

If you enable bandwidth utilization visualization in your map, the links will be colored according to these thresholds.

View Fault Information for Devices and Links

If a device or link has an alarm associated with it, an alarm badge is displayed on the device icon or on the link in the topology map. The color of the alarm badge corresponds with the alarm severity—minor (yellow), major (orange), or critical (red)—and matches the alarms displayed in the Alarm Browser.

For groups, the alarm badge represents the most severe alarm that is currently active for any of the group members.

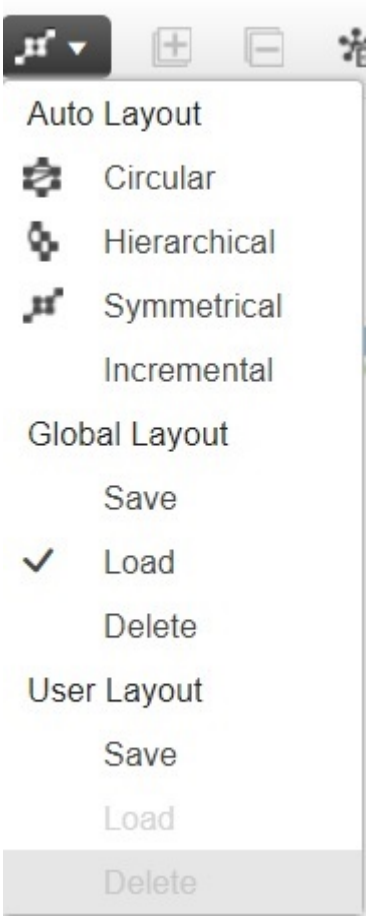
Link-related alarms, such as Link Down, generate an alarm badge on the relevant link in the topology map. After the link up alarm is received, the link alarms and corresponding badges are cleared.

See Alarm Severity Icons, on page 251 for more information.

Change the Layout of a Network Topology Map

When you first open the topology map, it is displayed according to the default global layout. The global layout can be changed by users with network topology "edit" privileges. Any changes you make in the map are maintained for the current browser session only, meaning that when you next open the map, the global layout will be applied. If you want your own map layout to be preserved for future sessions, you can save your layout. Your saved layout overrides the global layout.

Click the **Layout** icon in the topology toolbar to access the layout options.



- A checkmark indicates which layout is currently being used. For example, a checkmark next to "Load" under Global Layout indicates that the global layout is currently being used.
- If you move devices around in the map and you want to save the new layout as the global layout for all users, click **Save** under **Global Layout**. This option is only available for users with network topology "edit" privileges.
- If you move devices around in the map and you want to save your own layout for the next browser session, click **Save** under **User Layout**.

- If the global layout is being used and you want to use your own saved layout, click **Load** under **User Layout**.

You can specify how the devices and other network elements (such as labels, nodes, and the connections between them) are arranged in the topology map by dragging them to the required position in the map or by selecting one of the predefined options:

Procedure

	Command or Action	Purpose
Step 1	Symmetrical (default)—Maintains the symmetry that is inherent in the topology. This ensures that adjacent nodes are closer to each other and prevents node overlapping.	
Step 2	Circular—Arranges the network elements in a circular style highlighting the clusters inherent in the network topology.	
Step 3	Hierarchical—Ensures that the dependencies on the relationships and flows between elements are maintained.	
Step 4	Incremental—Maintains the relative positions of specific elements while adjusting the positions of newly added elements. Use this layout to re-render nodes/links and to clean up overlaps.	

Add a Background Image to the Network Topology

A background image can be applied to the topology map for any selected group. This is useful if, for example, you want to group your network according to geographic location. A sub-group can have a different image from its parent group. For example, you could apply a country map to one group and state maps to its sub-groups. Background images are saved per group and per user.

When a background image is applied, zoom functionality is supported and devices maintain their location on the image as you zoom in and zoom out.

The system provides some predefined images that you can select as background images. Alternatively, you can use your own custom background images.

Before you begin

When adding a custom background image, follow these guidelines:

- The background image file must reside on the server in a directory that is covered by high availability (HA), meaning that it will be moved to the secondary server in the case of primary server failure.
- Images should be in .png or .jpg format (.png is recommended).
- The file size should be as small as possible because the time taken to render the map is directly proportional to the size of the image.

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 In the Network Topology window, click the **Add Background Image** icon in the topology toolbar. The Manage Group Background Image dialog opens.

Step 3 Choose the required group from the Select Group drop-down list.

Step 4 Choose **Predefined** or **Custom Image** from the Background Image drop-down list.

Step 5 For a custom image, click **Select Image** , navigate to the image file and double-click it. For a predefined image, select one of the displayed images.

Step 6 Click **Apply**.

Step 7 In the topology map, arrange the devices as required (devices are arranged randomly on the map).

Step 8 Save the new layout by choosing **Layout** > **Save Current Layout**.

Visualize and Trace Circuits/VCs

When working with circuits/VCs, it is very useful to see how a circuit/VC is deployed within the existing network topology. Cisco EPN Manager overlays the circuit/VC on an existing topology map, clearly indicating the endpoints and midpoints of the circuit/VC, the role of the endpoint (where relevant), and relevant fault information for the circuit/VC.

Few points to note regarding overlay functionality in the topology map are:

- To overlay a circuit on the topology map, select the circuit/VC in the Circuits/VCs tab on the left
- If the selected group does not contain all the devices participating in the circuit/VC, a popup is displayed asking if you want to switch groups to show the full overlay.
- Select the **Show Participating Only** check box to remove all devices from the map except for those participating in the selected circuit/VC.

Note This option is force checked when exceeding upper limit of 1500 devices during circuit overlay.

When you select the **Show Participating Only** option and the restore path has some constraint links/nodes, the maps network topology will show links and nodes which are not part of working path.

- You can overlay a device group on the logical map without losing context when you change or expand the device group.

See View and Manage Discovered/Provisioned Circuits/VCs, on page 619 for more information.

Display Routes of a Circuit

For optical and CEM circuits, MPLS-TE, and SR-TE services, you can display routes associated with a specific circuit.

To do this use the **Routes** drop-down menu in the topology toolbar. The Routes menu calculates the routes from the links within a service. You can also see more data about the circuit routes. For example, the working

path is represented with a 'W' label and the Protected path with a 'P' label on the links. See Display the Routes Associated With a Circuit, on page 642.

For Optical Channel (OCH) circuits, you can launch the Chassis View of a participating device and view the end-to-end physical route of the circuit. To do this, choose an OCH circuit for which you want to view the physical route. From the map, click any of the participating device to launch the Chassis View.

The Chassis View displays the physical routes of the circuit. The internal connections between the ports of the same card are displayed as dotted lines. Use the eye icon in the Chassis View to show or hide the physical routes, power levels, and span loss.

Note You can launch the Chassis view of participating device only in case of OCH circuits. This feature is not supported for other types of circuits or services.

Trace and Visualize the Full Route of a Circuit

You can do a full multi-layer trace of a circuit from the Network Topology window. See Trace and Visualize the Full Route of Circuits/VCs, on page 676 for more information.

Show Clock Synchronization Networks on a Network Topology Map

If Synchronous Ethernet (Sync-E) or Precision Time Protocol (PTP) clock synchronization is configured on the devices in your network, you can visualize the clock synchronization network on the topology map.

- The Sync-E overlay shows the topology and hierarchy of the sync-E network, including the primary clock and the primary and secondary clock inputs for each device. This allows the clock signal to be traced from any Sync-E enabled device to the primary clock or from the primary clock to a Sync-E enabled device.
- The PTP overlay shows the clock synchronization tree topology, the PTP hierarchy, and the clock role of each device in the tree - primary, boundary, subordinate, or transparent.

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click on the **Device Groups** button, select the required device group(s), and click **Load**.

Step 3 Click **Show** in the topology toolbar and choose **Technology**. Click the question mark icon for a description of what will be displayed on the map for each technology.

Note Bandwidth Utilization option should be disabled before choosing Technology.

Step 4 Select the required technology and click **OK**.

The clock synchronization network is shown as an overlay over the existing network in the map. The legend at the bottom right explains the notations used in the map for the selected technology.

Note If you select a different device group, the technology overlay will be removed.

Show Routing Networks on the Topology Map

Routing protocols used in your network can be graphically represented as an overlay on the topology map. Overlay of the following routing protocols is supported:

- OSPF:
  - OSPF overlay shows the different OSPF domains in the network and the links between them, which are labeled as inter-area OSPF links. The overlay shows the OSPF area ID to which each link belongs and the role of each router, for example, Area Border Router (ABR), Designated Router (DR), and so on.
  - OSPF overlay is supported on devices running IOS-XE (Cisco ASR 900 series routers, Cisco ASR 920 series routers, and Cisco NCS 4200 series devices) and devices running IOS-XR (Cisco ASR 9000 series routers and Cisco NCS 4000 series devices. For Cisco NCS 1010 devices, direct OSPF overlay cannot be seen on network topology, instead DWDM layer-OTS link is used to view the network overlay). OSPF overlay is also supported on XR-XE cross-platform devices.
- BGP:
  - The BGP overlay labels each device with the ID of the autonomous system to which it belongs and shows the links within and between autonomous systems.
  - If two connected routers belong to the same autonomous system, the link is an internal BGP link. If they belong to different autonomous systems, the link is marked as an external link.
  - Each unique autonomous system has a different color so that you can easily identify devices belonging to the same AS.
  - The overlay also marks the devices that serve as route reflectors or route clients.
  - BGP overlay is supported on Cisco ASR 920 routers, Cisco ASR 901 routers, Cisco ASR 901_10G routers, Cisco NCS 4200 series devices and Cisco ASR 9000 series routers.
- ISIS:
  - The ISIS overlay shows the devices (Intermediate Systems - IS) running ISIS as the Interior Gateway Protocol (IGP). On these devices, you can see a notation that indicates the IS type, the area ID, which identifies the different ISIS domains, and an indication if the device has a Designated Intermediate System (DIS). The notation shows the first 6 bytes of the NET address. Hovering over the notation displays a tooltip containing the complete NET address and the process ID.
  - The IS type can be L1 for intra-area routing, L2 for routing between areas, or L1L2 for intra-area and inter-area routing.
  - Each ISIS domain is represented in a different color.
  - A notation on the links in the ISIS network indicates the ISIS adjacency. For aggregated links where multiple adjacency types exist, multiple adjacency type notations will be shown on the link.

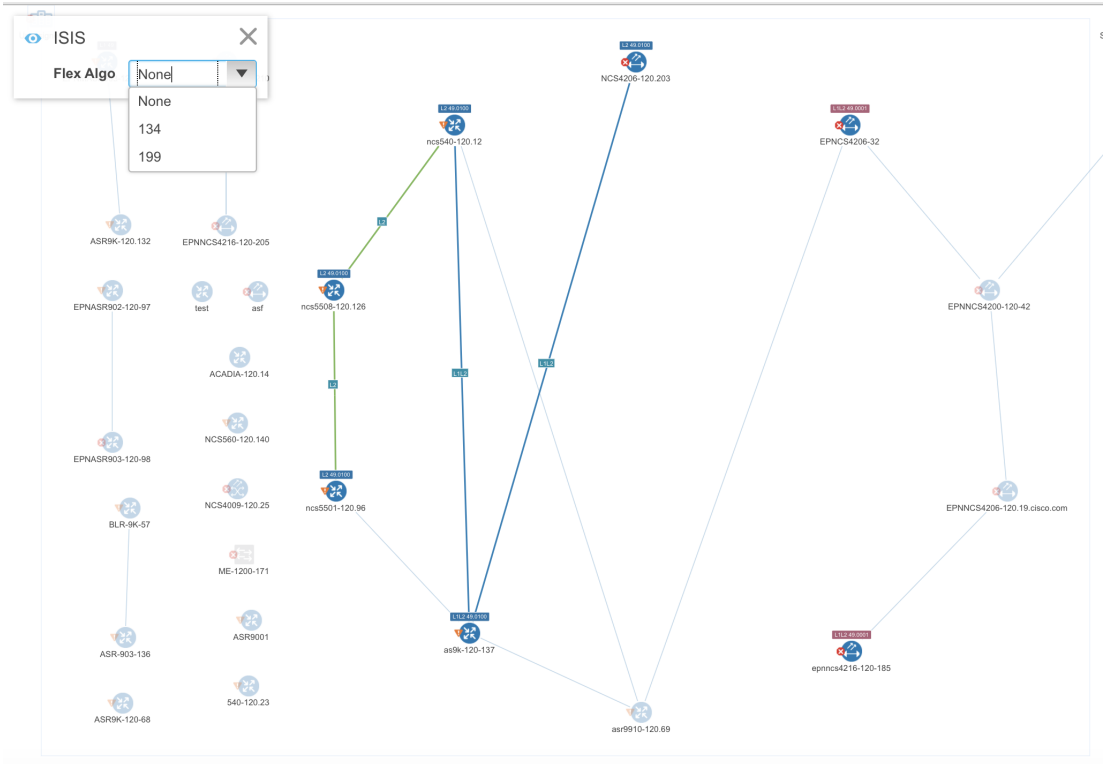
- Select a value from the **Flex Algo** drop-down list. After you select a value, Cisco EPN Manager updates the overlay to reflect only those devices that are configured with the specified Flex Algo value. Other unsupported devices (Cisco IOS-XE devices) and nonmatching IOS-XR nodes are grayed out.

Note Select **None** to revert to the default ISIS overlay.

- ISIS overlay is supported on devices running IOS-XE (Cisco ASR 903 routers, Cisco ASR 907 routers, and Cisco NCS 4200 series devices) and devices running IOS-XR (Cisco ASR 9000 series routers, Cisco NCS 4000 series devices). ISIS overlay for Flex Algo is supported on IOS-XR (Cisco ASR 9000 series routers, Cisco NCS 540 series routers, Cisco NCS 560 series routers, and Cisco NCS 5500 series devices).

Note DIS indication is presented on the device level and not in the context of a specific IS level.

The following is an example of an ISIS overlay in the map:



To show a technology overlay in the map:

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click on the **Device Groups** button, select the required device group(s), and click **Load**.

Step 3 Click **Show** in the topology toolbar and choose **Links**. Make sure that the map is showing the relevant types of link, for example, ISIS links, BGP links, and OMS links. In addition, if Bandwidth Utilization is enabled, disable it.

Step 4 Click **Show** in the topology toolbar and choose **Technology**. Click the question mark icon for a description of what will be displayed on the map for each technology.

Step 5 Select the required routing protocol and click **OK**.

The routing network is shown as an overlay over the existing network in the map. The legend at the bottom right explains the notations used in the map for the selected technology.

Note If you select a different device group, the technology overlay will be removed.

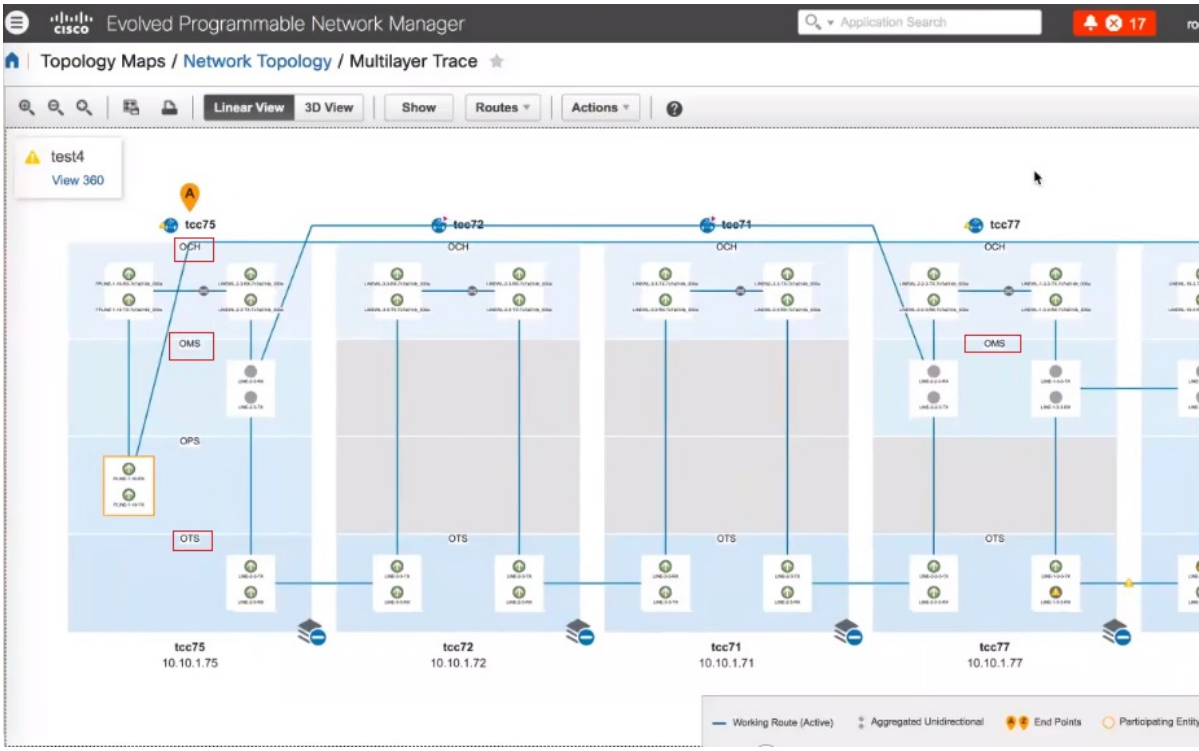
View OMS Links

In EPNM, view the auto discovered OMS links for ROADM devices that are connected by means of sequence of OTS links. You can view the multitrace view of the OMS links, Circuit/VCs 360* view, and the characteristics of OMS links and alarm link layers of OMS.

To view the multitrace view of OMS links:

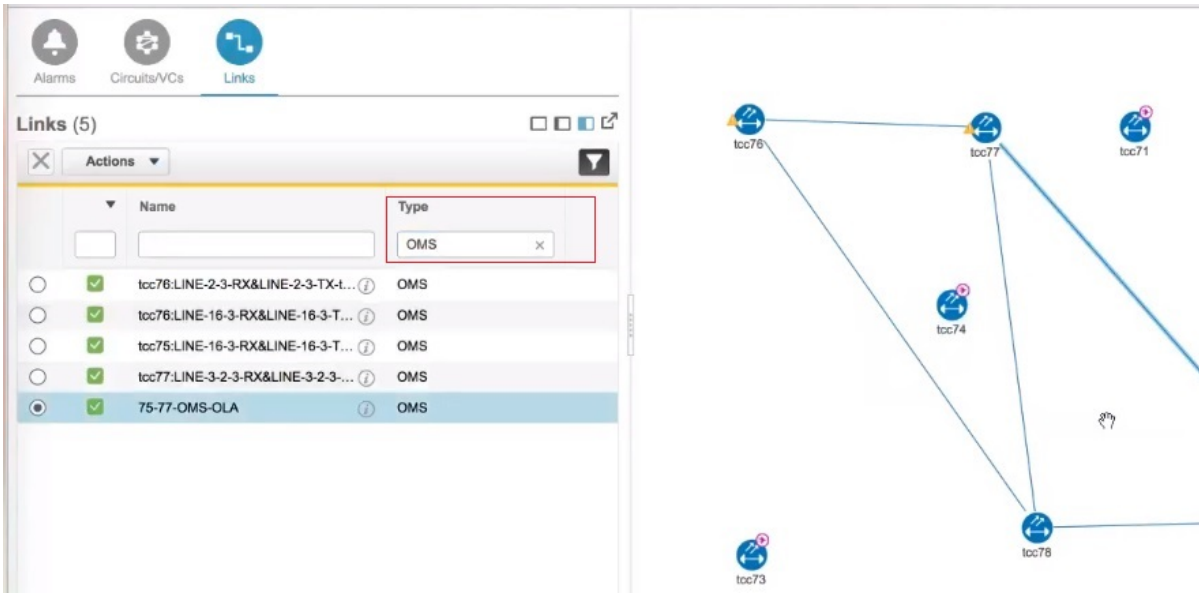
- Choose **Maps** > **Topology Maps** > **Network Topology**.
- Click **Circuit/VCs**, choose the device then click the **Multilayer Trace** link to view the connected links. For example, the following image shows the multitrace view of OMS links along with OCH and OPS link layers.

Figure 3: Multilayer Trace View



Use the **Type** filter to select and view only the OMS link and its network .

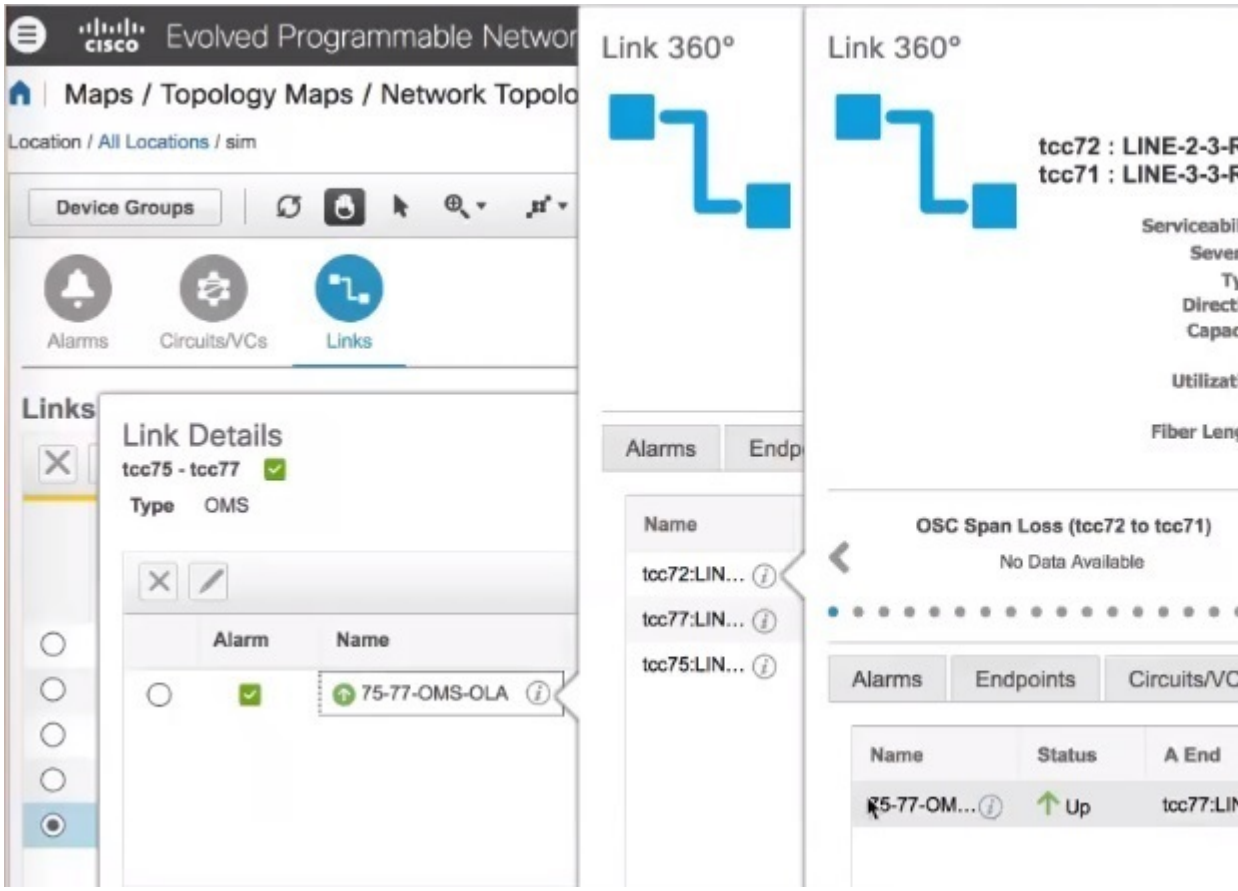
Figure 4: Choose OMS from Type Filter



To view the characteristics of the OMS link:

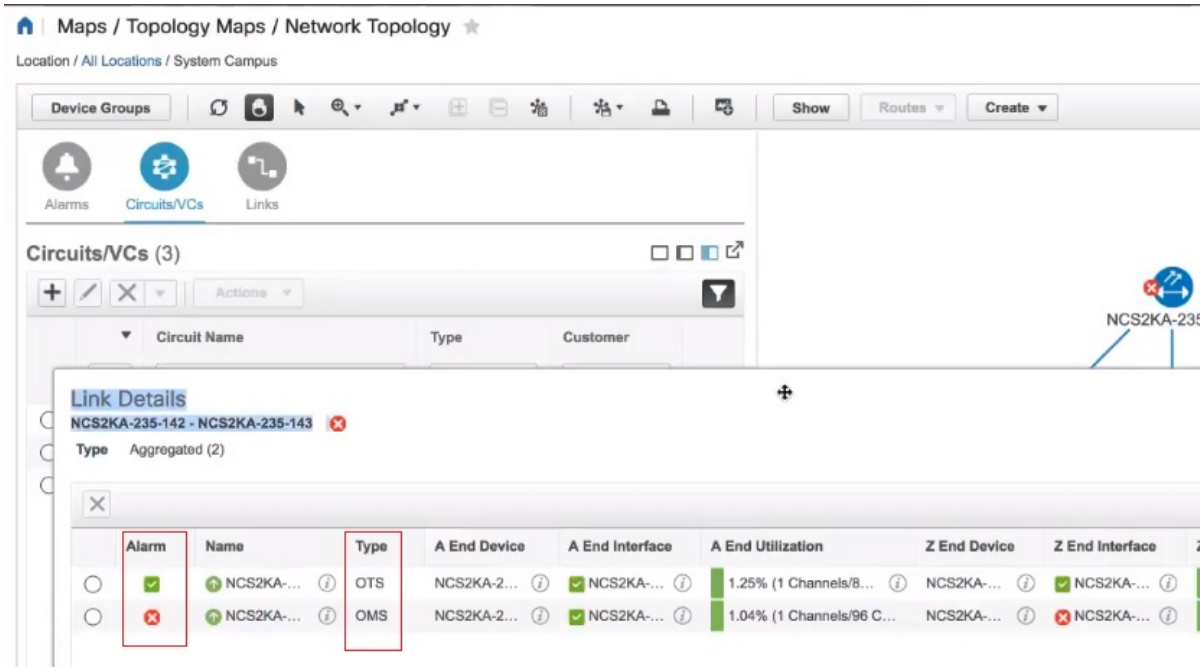
- Click the **Show** button and view where the OMS link is used in the **Link Details** dialog box. For the selected OMS link type , view the endpoints , the planned circuit VCs, if any and the sequence of OTS link details.

Figure 5: Link Details and Link 360* View



- Click the *i* icon next to the OTS link name to view the Link 360* view of the OMS link type.
- View the alarm link layers for OMS links.

Figure 6: Link Details with Alarms



Locate the SR Path Between Devices on the Topology Map

To find the active SR paths between SR supported devices on the topology map:

Step 1 Click on the SR supported device from which you want to find the SR path. A popup appears showing the basic device information and alarm information for the device.

Step 2 Click **Show SR Path**. The Show SR Path dialog opens.

Step 3 To select the endpoint, click on the SR supported device to which you want to find the SR path. The endpoint field gets populated with the details of the selected device.

Note Error message is displayed if the selected device does not support segmented routing.

You can also select a device by entering the device name in the field or selecting it from the drop down list.

Step 4 Click **OK**. The SR path gets highlighted on the topology map for the selected devices.

View Your Network on a Geographical Map (Geo Map)

- Geo Map Overview, on page 204
- Geo Map Setup, on page 206
- Identify Which Devices are not Showing on the Geo Map (Unmapped Devices), on page 206

- Place Unmapped Devices on the Geo Map, on page 206
- Change the Location of a Device on the Geo Map, on page 207
- Change the Location of a Device in a Cluster, on page 208
- Remove a Device from the Geo Map, on page 208
- Identify Which Devices are not Showing on the Geo Map (Unmapped Devices), on page 206
- Search for a Device in the Map, on page 177
- Locate the SR Path Between Devices on the Geo Map, on page 213

Geo Map Overview

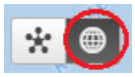
The geo map enables you to position your network devices on a world map and monitor them within their geographical context. The displayed world map is either imported by accessing the map provider's site over the Internet (online mode) or from locally installed map resources (offline mode).

Note When working with the geo map in online mode, a connection to the Internet is required from each client or from the Cisco EPN Manager server if it is being used as a proxy.

The geo map is accessed via the topology map. To open the geo map:

Step 1 In the left sidebar, select **Maps** > **Topology Maps** > **Network Topology**

Step 2 Click on the Geographical Map toggle button in the top right corner of the map.



About the geo map:

- You can switch back and forth between the topology map and the geo map using the toggle buttons in the top right corner of the map.
- The geo map displays devices for which GPS coordinates have been defined. Devices that do not have GPS coordinates do not appear on the geo map and are called “unmapped devices.” See Place Unmapped Devices on the Geo Map, on page 206.
- You can click on a device in the geo map to see alarms, basic information, location coordinates and civic location (if it has been defined for the device).
- For optical devices that support GPS location configuration (NCS 2000 devices), any change that is made to the device's location in the geo map is synched with the device and vice versa (location changes made on the device itself will be reflected in the geo map).
- GPS coordinates are shown in DMM format (degrees and decimal minutes) but users can define GPS coordinates in DMM, DD (Decimal Degrees), or DMS (Degrees, Minutes, and Seconds) formats.

- If there are no devices on the geo map, the full world map is shown. If there are devices in a specific area, only that area of the world will be shown. The geo map shows only the portion of the world map that contains devices.
- As in the topology map, the geo map shows the devices in the selected device group. The device group selection is synchronized between the topology map and the geo map such that if you change the selection in one map, it will change in the other map as well.
- If there is a device group that has a defined geographical location within the selected device group it will be represented in the geo map with a device group icon. If the device group does not have a geographical location, its contained devices will be shown individually in the geo map. See Device Groups in the Geo Map, on page 205 for more information.
- The geo map groups devices that are close to one another geographically in clusters, represented by a cluster icon with a number indicating the number of devices in the cluster. Zoom in to see the individual devices. See Identify the Members of a Cluster, on page 209.
- As in the topology map, you can show a circuit/VC in the geo map. However, when initiating provisioning actions such as creating a circuit/VC or modifying a circuit/VC, the view will switch to the topology map.

Device Groups in the Geo Map

In addition to individual devices, the geo map shows device groups that have a defined location, for example, devices in a building at a specific address.

Take the following into consideration when viewing groups in the geo map:

- Only location-type device groups can be shown in the geo map, and they are only visible if they have a defined geographical location. The location is defined in the device group properties. To create or edit a location device group and define the geographical location of the group, go to **Inventory > Group Management > Network Device Groups**. See Create Location Groups, on page 77 for more information.
- Group members inherit the location of the group.
- If a group's location is the same as other devices/groups, it will be included in a cluster. The number displayed on the cluster icon represents the total number of devices in the cluster (including devices contained in groups).
- If there are alarms on any of the devices within a group, the highest severity alarm icon will be displayed on the device group icon.
- Click on the location group icon to see a panel containing information about the group, including its name, GPS coordinates, and alarm information. If civic location information is defined for the group, it will also be shown in this panel. Click on the **Show Members** link in the panel to show a list of the devices and sub-groups that belong to the group. Alternatively, double-click on the location group icon to achieve the same results.
- If a group member device is given a geographical location, the device will be shown on the geo map as an individual device and alarms will be shown on the device itself, not on the group. It is preferable to have all devices in a geographical location group inherit the GPS coordinates of the group in order to retain the significance of the group's location.

Geo Map Setup

The system is set up by default to get the map tiles from a specific Mapbox URL through a direct Internet connection from the client or via the EPN Manager server which acts as a proxy. If required, you can use a different map tiles provider by providing a specific URL. Both of these options require an Internet connection. If you do not have an Internet connection, you can install the map resources locally and specify that you want the system to use the local map resources, which means that you are effectively working in offline mode.

The geo map setup can be managed in the System Settings. In the left navigation pane, select **Administration** > **Settings** > **System Settings** > **Maps** > **Network Topology**.

In the Network Topology page, you can do the following:

- Enable/disable the geo map. By default, geo map is enabled, meaning that all clients will have the geo map functionality. You can deselect the **Enable geo map** checkbox to disable the functionality.
- Identify the source for the map tiles (using an Internet connection). The default map tiles provider is Mapbox. If you are working with another map tiles provider, you need to provide the URL for map tiles access. Be sure to request the exact format of this URL from the map tiles provider. Select **Custom** in the Map Provider dropdown list and enter the URL. Note that the geo map functionality has not been tested with map tiles from providers other than Mapbox.
- Make the Cisco EPN Manager server a proxy for accessing the Internet to retrieve the map tiles. For security reasons, you might not want direct Internet access from each client. If you enable the **Via management application proxy** check box, Internet access to the map provider URL is via the Cisco EPN Manager server, not directly via the clients.
- Specify that you want to display the geo map using installed map resources that do not require a connection to the Internet. Select **Installed Map Resources** in the Map Provider dropdown list. Refer to the Cisco Evolved Programmable Network Manager Installation Guide for instructions on how to install the map resources.

Identify Which Devices are not Showing on the Geo Map (Unmapped Devices)

For any selected device group, only the devices that are defined with GPS coordinates will automatically be shown on the geo map. When you switch to the geo map or when you select a different device group, a popup message will indicate how many unmapped devices there are, meaning how many devices that do not have coordinates and therefore do not appear on the map.

To identify which devices are not being shown on the geo map, click the **Unmapped Devices** button above the map.

Place Unmapped Devices on the Geo Map

You can either drag and drop unmapped devices onto the required location on the geo map or you can specify the GPS coordinates to define the device's location on the geo map.

GPS coordinates can be specified in any of the following formats:

- Degrees and decimal minutes (DMM): 41 24.2028, 2 10.4418
- Decimal degrees (DD): 41.40338, 2.17403
- Degrees, minutes, and seconds (DMS): 41°24'12.2""N 2°10'26.5""E

Note When using DMS format, please use a double quotation mark ("") to indicate the seconds.

To place unmapped devices on the geo map:

Step 1 In the left sidebar, select **Maps** > **Topology Maps** > **Network Topology**

Step 2 Click on the Geographical Map toggle button in the top right corner of the map.

Step 3 Click the Unmapped Devices button above the map.

Step 4 In the Unmapped Devices panel on the right, either:

a) Drag and drop a device onto the map or select multiple devices and drag and drop them onto the map.

b) Select the device(s) you want to place on the map and click **Set Location**. In the displayed dialog, specify the GPS coordinates, for example, Latitude 59.623325, Longitude-103.535156. Click **Place Device**.

Note If you select multiple devices, they will be consolidated into a cluster and placed on the same location on the map. The cluster icon indicates how many devices the cluster contains.

Change the Location of a Device on the Geo Map

To move a device to a different location on the geo map, you need to open the Edit Location dialog and then either drag the device to the required location on the map or set the coordinates manually. If the device is in a cluster, you must open the cluster to view the devices and then change the location of the device.

GPS coordinates can be specified in any of the following formats:

- Degrees and decimal minutes (DMM): 41 24.2028, 2 10.4418
- Decimal degrees (DD): 41.40338, 2.17403
- Degrees, minutes, and seconds (DMS): 41°24'12.2""N 2°10'26.5""E

Note When using DMS format, please use a double quotation mark ("") to indicate the seconds.

To change the location of a device:

Step 1 Click on the device on the geo map. A popup appears showing basic device information and alarm information for the device.

Step 2 From the **Actions** drop-down list, select **Edit Location**. The Edit Location dialog opens.

Step 3 Drag the device to the required location or change the GPS coordinates as required.

Step 4 Click **Save**.

Change the Location of a Device in a Cluster

Devices that are very close to each other in location are grouped in a cluster on the geo map. You can change the location of one or more of the devices in the cluster. The device will be removed from the cluster and will appear on the geo map as an individual device.

To change the location of a device in a cluster:

Step 1 Click on the cluster in the geo map. A popup appears showing basic information for the cluster.

Step 2 Click **Show Devices**. A panel is displayed to the right of the map and lists all the devices in the cluster.

Step 3 In the panel on the right, either:

a) Drag and drop a device onto the map or select multiple devices and drag and drop them onto the map.

b) Select the device(s) you want to place on the map and click **Set Location**. In the displayed dialog, specify the GPS coordinates, for example, Latitude 59.623325, Longitude-103.535156. Click **Place Device**.

The device(s) will be removed from the cluster and placed in the specified location on the map.

Remove a Device from the Geo Map

If you no longer want to display a device on the geo map, you can remove it. The removed device will appear in the Unmapped Devices list.

To remove a device from the geo map:

Step 1 Click on the device on the geo map. A popup appears showing basic device information and alarm information for the device.

Step 2 From the **Actions** drop-down list, select **Edit Location**. The Edit Location dialog opens.

Step 3 In the Edit Location dialog, click **Remove Location**.

Remove a Clustered Device from the Geo Map

Devices within clusters can be removed from the geo map. You can remove an individual clustered device or you can remove multiple devices in the same cluster at one time. The removed device(s) will appear in the Unmapped Devices list.

To remove clustered devices from the geo map:

Step 1 Click on the cluster containing the device(s) you want to remove. A popup appears showing basic device information and alarm information for the device.

Step 2 Click **Show Devices**. A list of the devices contained in the cluster is displayed.

Step 3 Select the device(s) you want to remove.

Step 4 Click **Set Location**.

Step 5 In the displayed dialog, click **Remove Location**.

Step 6 Click **Yes** in the warning message informing you that the devices will be moved to the Unmapped Devices list.

Identify the Members of a Cluster

A cluster is formed when two or more devices or device groups are located close to one another on the map. The cluster is represented on the geo map by a circle with a number in its center, indicating the number of devices in the cluster (including individual devices and devices within groups). Zoom in to see the individual cluster members on the map.

Note If cluster members are very close to each other (approximately 8 meters apart or less), zooming in will not show the individual devices/groups. Follow the procedure below to see the individual members of the cluster.

To see a list of the devices/groups in a cluster:

Step 1 Click on the cluster icon.

Step 2 In the displayed popup, click **Show Members**. The devices or device groups contained in the cluster are listed in the panel to the right of the map. If the cluster contains groups, you can drill down to see the devices in the group. Use the navigation links at the top of the dialog to return to the previous list.

Step 3 You can change the location of a device by dragging it from the list onto the map or by clicking **Set Manually** and specifying new coordinates.

Search for a Specific Location in the Geo Map

You can search for a specific location in the geo map, for example, a state, country, town, or a specific address. If you enter a keyword in the search box, the results will show all locations that contain that keyword, down to the level of a specific street. You can then select the required location in the search results to pinpoint it in the map.

Note Internet connectivity is required to perform this location search.

To search for a specific location in the geo map:

Step 1 Click the **Search** icon in the toolbar.

Step 2 Type the full or partial result in the search text box and press **Enter**.
The Address tab in the search results panel lists locations that match your search.

Step 3 Select a location in the search results.
The map pans and zooms to the specified location and a marker on the map indicates the exact location.

Location Filter in the Geo Map

To use the location filter in the geo map:

Step 1 Go to the **Map** > **Topology Maps** > **Network Topology**, click the **Show** button and select **Location**.

Step 2 In the **Location** pop-up window, check the **Enable Filter** option. Specify values for any of the following fields:

- *Civic location*: any civic location, regardless of the location the device.
- *Latitude/Longitude*: location coordinates (you can also click on the map, and the values are automatically populated)
- *Location by Device name*: name of the device (from the list of devices currently displayed in Geo Map.

Step 3 Specify value for the **radius**, and all devices within the prescribed search area are displayed.

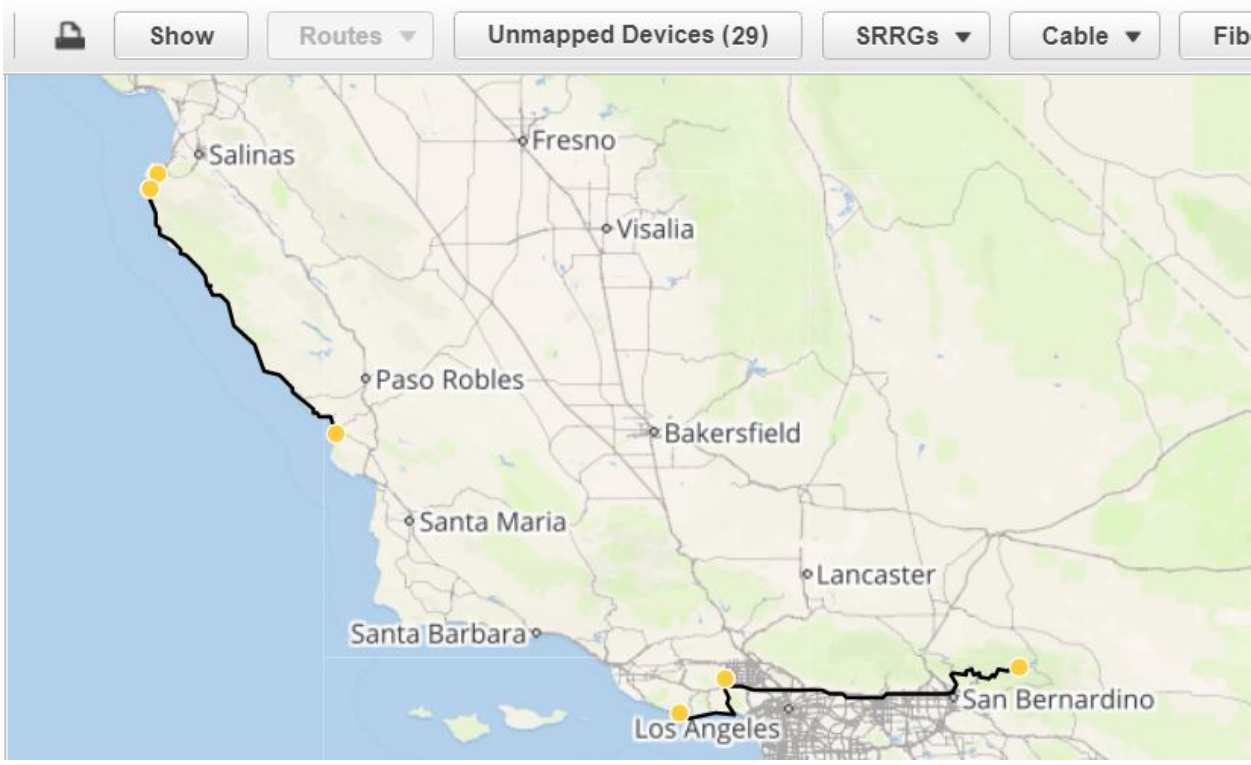
Step 4 Once completed, click **Save**.

View and Manage Optical Fiber Paths in the Geo Map

To view optical fibers in the geo map, you must create a KML file with the location data for the fibers and import it into Cisco EPN Manager. For information about importing fiber location data, see Import Location Data from a KML File, on page 213.

After you import a KML file that contains fiber location data, the fibers are shown on the geo map. If you do not want to see them on the map, go to **Show** > **Links** and uncheck **Fiber** under Physical Layer links.

Optical fibers are represented as follows in the geo map:



See Manage Fiber Paths, on page 211 and Associate Links to Fibers, on page 212 for information about editing/deleting fibers and associating fibers to links.

Manage Fiber Paths

Fiber paths that are displayed in the geo map can be edited, deleted, or associated to links in the Fiber Management dialog. Click the **Fibers** button in the geo map toolbar to open the Fiber Management dialog.

Note the following:

- The Fiber Management dialog lists fibers that are currently visible in the map only. If you cannot see the fibers in the geo map, they will not appear in the Fiber Management dialog. Set up your geo map so that the fibers you want to manage are being displayed.
- When you select a fiber in the Fiber Management dialog, the selected fiber is highlighted in purple in the geo map. If the fiber is associated with a link, the link will also be highlighted in purple in the map. When you click on a fiber in the geo map, the fiber is selected in the Fiber Management dialog.
- To show additional details about a specific fiber, click the arrow next to the fiber name to show the fiber description.
- You can edit the fiber name, length (in km), and description. To edit a fiber, select it in the list and click the **Edit** button. Click **Save** when you have completed your edits.
- To delete fibers, select the required fibers and click the **Delete** button.
- The Associated Link column shows the link to which the fiber is associated (if any). You can disassociate the link if necessary by selecting the fiber and clicking the Remove Fiber to Link Association icon above the table. See Associate Links to Fibers, on page 212 for more information.

Associate Links to Fibers

A fiber can be associated to an OTN or OTS link so that you can visualize both the fiber and its associated link on the map. To associate a fiber to a link, you must populate a KML file with the necessary information and then import the KML file into the system.

A KML template that outlines the format for providing fiber-link associations can be downloaded and then imported after you have added the required information.

To associate a link to a fiber:

Step 1 Download the KML template that contains the correct KML format and instructions for fiber-link associations:

- Click the **Import** icon in the geo map toolbar and choose **KML**.
- Download the KML template by clicking the link at the bottom of the displayed dialog.
- In the KML file, locate the folder called "Links association info". This folder contains the format and instructions for creating a fiber-link association.

Step 2 Enter the required information in the KML file, save it, and then import it into the system. See Import Location Data from a KML File, on page 213.

Step 3 In the geo map, check that your fibers are displayed, then click on **Fibers** in the toolbar. In the Fiber Management dialog, the links should show up in the Associated Links column. You can remove the link association by selecting the fiber and clicking the Remove Fiber to Link Association icon above the table.

Visualize Circuits/VCs on the Geo Map

The circuit/VC overlay functionality in the geo map is very similar to overlay in the topology map. However, because of some differences in the functioning of the maps, a few items regarding overlay functionality in the geo map need to be noted:

- To overlay a circuit on the geo map, select the circuit/VC in the Circuits/VCs tab on the left, as you would in the topology map.
- Select the **Show Participating Devices Only** check box to remove all devices from the map except for those participating in the selected circuit/VC.
- Click the **Participating Devices** link to show a list of all the devices participating in the circuit/VC. The list shows the role of the devices, for example, A-side and Z-side, and you can change the location of the devices or remove them from the map.
- If a participating device is in a cluster on the geo map, the badge denoting the role of the device is shown on the cluster icon. Zoom in to see the individual devices so that you can see exactly which device the role badge is marking. Alternatively, click on the **Participating Devices** link to see all the devices and their roles in the circuit/VC.
- If some of the participating devices are not currently displayed on the map, a message will be displayed and will enable you to open the list of unmapped devices. You can place them on the map by dragging and dropping the devices or click **Set Location** and enter their GPS coordinates.

Locate the SR Path Between Devices on the Geo Map

To find the active SR paths between devices on the geo map:

Step 1 Click the SR supported device from which you want to find the SR path. A pop-up appears displaying the basic device information and alarm information for the device.

Step 2 From the **Actions** drop-down list, select **Show SR Path**. The Show SR Path dialog opens.

Step 3 To select the endpoint, click the SR supported device to which you want to find the SR path. The endpoint field gets populated with the details of the selected device.

Note Error message is displayed if the selected device does not support segmented routing.

You can also select a device by entering the device name in the field or selecting it from the drop-down list.

Step 4 Click **OK**. The SR path gets highlighted on the geo map for the selected devices.

Import Location Data

In addition to manually placing devices on the geo map, you can specify the coordinates of devices or fibers in an external file and then import the file. The system reads the coordinates from the file and places the devices/fibers on the map. This is useful for locating items on the map in bulk or for transferring location data from another system. You can also export your existing locations from the geo map, make changes, and then import the data back into the system.

You can import device and fiber path locations and manually-created managed links from a KML file.

For the KML file format you can download a template from the GUI which will guide you on the format in which you need to enter the information so that the system can read it. To download the template, click on the Import Locations icon above the geo map, and click on the template link.

See Import Location Data from a KML File, on page 213 for more information.

Import Location Data from a KML File

Keyhole Markup Language (KML) is a file format used to display geographic data in two- or three-dimensional maps or in Earth browsers like Google Earth. KML is based on the XML standard and uses a tag-based structure with nested elements and attributes. You can create a KML file with your device and fiber path location data and import it in order to place your devices and fibers on the geo map. The following location data can be included in the KML file:

- Device location data
- Fiber location data
- Fiber to link associations
- Manually-created managed links. After import, the managed links will be displayed in the topology map and in the geo map (if both endpoints of the managed link are "mapped" in the geo map).

A template is provided to guide you as to the required format in which to enter information within the KML file.

Note Coordinates must be entered in Decimal degrees (DD) format, for example, 41.40338, 2.17403.

Following is an example of the KML format for device locations:

```
<Placemark>
 <name>454A-234-157</name>
 <Point>
  <coordinates> -121.930938,37.411522</coordinates>
 </Point>
 <ExtendedData>
  <Data namename="nodeIpAddress">
   <value>10.56.23.47</value>
  </Data>
 </ExtendedData>
</Placemark>
```

Following is an example of the KML format for fiber paths:

```
<Placemark>
 <name>Fiber-1</name>
 <description>Fiber-1 long description</description>
 <LineString>
  <coordinates> -121.930938,37.411522,0.0 -121.931405,37.413011,0.0 -121.929364,37.413588,0.0
 -121.930973,37.414602,0.0
  </coordinates>
 <LineString>
</Placemark>
```

Following is an example of the KML format for fiber-link associations, where you must:

- Define one link association per folder, with the name "linkAssociation".
- Specify the segments of the fiber in the sequence that follows the A to Z path of the link to be associated.
- Specify the IP address of the A and Z sides of the link to be associated.

```
<Folder>
 <name>Links association info</name>
  <Folder>
   <name>linksAssociation</name>
   <description>OTS link-1</description>
   <ExtendedData>
    <Data> name="segments">
     <value>Fiber-1,Fiber-1-to-2-segment,Fiber-2</value>
    </Data>
    <Data> name="nodeAIpAddress">
     <value>10.56.23.47</value>
    </Data>
    <Data> name="nodeZIpAddress">
     <value>2001:cdba:0000:0000:0000:0000:3257:9652</value>
    </Data>
    <Data> name="nodeAInterfaceName">
     <value>LINE-2-17-3-TX</value>
    </Data>
    <Data> name="nodeZInterfaceName">
     <value>LINE-1-1-3-TX</value>
    </Data>
    <Data> name="linktype">
     <value>OTS</value>
    </Data>
```

```
   </ExtendedData>
  </Folder>
</Folder>
```

Following is an example of the KML format for fiber-link associations, where you must:

- Define one link association per folder, with the name "linkAssociation".
- Specify the segments of the fiber in the sequence that follows the A to Z path of the link to be associated.
- Specify the IP address of the A and Z sides of the link to be associated.

```
<Folder>
 <name>Links association info</name>
  <Folder>
   <name>linksAssociation</name>
   <description>OTS link-1</description>
   <ExtendedData>
    <Data> name="segments">
     <value>Fiber-1,Fiber-1-to-2-segment,Fiber-2</value>
    </Data>
    <Data> name="nodeAIpAddress">
     <value>10.56.23.47</value>
    </Data>
    <Data> name="nodeZIpAddress">
     <value>2001:cdba:0000:0000:0000:0000:3257:9652</value>
    </Data>
    <Data> name="nodeAInterfaceName">
     <value>LINE-2-17-3-TX</value>
    </Data>
    <Data> name="nodeZInterfaceName">
     <value>LINE-1-1-3-TX</value>
    </Data>
    <Data> name="linktype">
     <value>OTS</value>
    </Data>
   </ExtendedData>
  </Folder>
</Folder>
```

To import location data from a KML file:

Step 1 Click the **Import** icon in the geo map toolbar and choose **KML**.

Step 2 Optionally download the KML template by clicking the link at the bottom of the displayed dialog.

Step 3 Create a KML file and enter device/fiber/link data using the format and information in the template as a guide. Save the KML file.

Step 4 In the Import KML dialog, browse to the saved KML file and click **Import**. The devices and fibers will be placed on the geo map in the locations you specified. Managed links will be displayed in the topology map. To see the imported managed links in the geo map, make sure that the devices on either side of the link are mapped in the geo map.

Export Location Data from the Geo Map

You can export location data for devices, fibers, fibers with link associations, and manually-created managed links from the geo map to a KML file. Once you have the data in a KML file, you can edit it as required and then import it back into the geo map.

Note Fiber location data cannot be exported together with the other location data - it must be exported in a separate operation.

Step 1 Click the **Export KML** icon in the geo map toolbar.

Step 2 In the Export Options (KML) dialog, select the location data you want to export.

Note You can select Device Geo Location, Managed Links, Unmanaged Links, Unmanaged Devices, Unmanaged Networks, Associated Fibers, and Unassociated Fibers. If you select Unassociated Fibers, the other options will be disabled because these fibers must be exported independently of the other location data.

Step 3 Click **Export**. A KML file with your selected location data is created.

Sync Offline Devices

You can configure to sync the offline devices or device groups based on the offline time threshold. Syncing of offline devices is disabled by default. Syncing of offline devices enables automatic device sync after the recovery of reachability failure. You cannot select only the devices of parent group without all child groups. On selecting any one of the child groups, the parent group will not be considered as selected. To address this scenario, you can create new child groups which can contain devices of the parent group. To configure when the sync happens for the offline devices:

Step 1 Go to **Administration > Settings > System Setting > Inventory** and select **Sync Offline Devices**.

Step 2 Use the **Select** button to choose between By Group or By Device.

Step 3 Select the device group or devices that you want to configure for syncing.

Step 4 Set the **Offline Threshold Time** from the hours and minutes drop-down list.

Step 5 Click **Save**.

Manage Shared Risk Resource Groups (SRRGs) in the Geo Map

Note This feature is supported on optical devices and links only, specifically NCS 2000 and NCS 4000 devices and OTS, OTU and OCH links.

A Shared Risk Resource Group (SRRG) is a set of devices and links that share a common resource, which if it fails, would affect all the devices and links in the group and the circuits in which they participate. The

devices and links in the group share the same risk of failure and are therefore considered to belong to the same SRRG. For example, links sharing a common fiber are said to be in the same SRRG because a fault with the fiber might cause all links in the group to fail.

Each SRRG has a 32-bit numeric identifier. For devices, the SRRG is configured on the global device level. For links, the same SRRG is configured on the A-side and Z-side interfaces.

The following SRRG functionality is available from the geo map, from the **Shared Risks (SRRGs)** button above the map:

- Visualization of the devices and links on which SRRGs have been configured.
- User-defined naming of an SRRG so that it is easier to identify than a numeric identifier.
- Creation of new SRRGs that can be assigned to SRRG resource pools.
- Cross-launch to the system settings window where you can create and manage SRRG pools and pool types.

When managing SRRGs, the map is filtered to show only devices that support SRRG.

For more information, see:

- About SRRG Pools and SRRG IDs, on page 217
- View Assigned and Unassigned SRRGs, on page 218
- Manage SRRG Assignments, on page 219
- Create and Manage SRRG Pools Types and Resource Pools, on page 220

About SRRG Pools and SRRG IDs

Using SRRG pool types and resource pools, SRRGs can be grouped into categories for identification and ID allocation purposes. Each pool type has a range of SRRG IDs. You can create multiple SRRG resource pools of a specific pool type, each with a range of SRRG IDs that is within the range defined for the pool type. When you create a new SRRG for devices or links, you can assign it to a specific SRRG pool type and resource pool. The ID for the new SRRG will be created from the ID range of the selected resource pool.

Note Configlet Access permissions are required to manage SRRG pool types and pools.

See Create and Manage SRRG Pools Types and Resource Pools, on page 220 for more information.

Pool Types

Before creating SRRG resource pools, you must create pool types. Pool types allow you to create categories of SRRGs according to your network.

There are 15 available pool types plus one pool type which is reserved. Each pool type has a range of IDs. The following table provides an example of SRRG pool type definitions:

Pool Type ID	Binary	Pool Type Name	Range Start	Range End
0	0000	Central Office	0	1048575
1	0001	ROADM Node	1048576	2097151

Pool Type ID	Binary	Pool Type Name	Range Start	Range End
2	0010	ROADM Degree	2097152	3145727
3	0011	ROADM Add/Drop	3145728	4194303
4	0100	Switch Node	4194304	5242879
5	0101	Link	5242880	6291455
6	0110	Card	6291456	7340031
7	0111	Future	7340032	8388607
8	1000	Fiber Duct/Conduit	8388608	9437183
9	1001	Future	9437184	10485759
10	1010	Future	10485760	11534335
11	1011	Future	11534336	12582911
12	1100	Future	12582912	13631487
13	1101	Future	13631488	14680063
14	1110	Future	14680064	15728639
15	1111	EPNM Preserved Global	15728640	16777215

SRRG Resource Pools

After you have created pool types, you can create resource pools of a specific type. Each resource pool can have a range of IDs that is within the pool type's range. The pool ranges cannot overlap with one another.

You can assign new SRRGs to a specific resource pool. The SRRG's ID will be taken from the range defined for the resource pool.

The SRRG pool's identifier is 32-bit number which is made up of the following:

- **Bits 0-1:** Reserved. It will be set to 00
- **Bit 2:** Indicates that the SRRG is configured using Cisco EPN Manager. It will be set to 1.
- **Bits 3-7:** The groups/regions selected for the resource pool
- **Bits 8-11:** Pool type ID
- **Bits 12-31:** Pool ID range

View Assigned and Unassigned SRRGs

You can view a global list of the SRRGs configured on the managed devices. Since these SRRGs were discovered by the system or user-defined on specific devices or links, they are all "assigned" SRRGs. You can also see unassigned SRRGs. SRRGs can only be deleted from the system if they are unassigned.

Note Ensure that you unassign a SRRG or delete a SRRG on a device from Cisco EPN Manager only. Doing so from the device will not unassign or delete the SRRG from ENE in Cisco EPN Manager.

Each SRRG has a numeric ID that cannot be changed but you can assign a label to the SRRG to provide a more easily identifiable name.

You can select an SRRG to show the devices/links to which it is assigned in the geo map.

To view and label SRRGs:

Step 1 In the left sidebar, select **Maps > Topology Maps > Network Topology**.

Step 2 Click on the Geographical Map toggle button in the top right corner of the map.

Step 3 Click the **Shared Risks (SRRGs)** button above the map and select **View and Name**. The Shared Risk Resource Groups dialog is displayed. It contains two tabs showing assigned and unassigned SRRGs. Note that when viewing SRRG assignments, your device group selection is changed to the default All Locations group.

Step 4 Select a SRRG to view it in the geo map. The devices and links on which the SRRG is defined will be highlighted in the map.

Step 5 To rename a SRRG, click in the SRRG Label column alongside the relevant SRRG ID, type in the required unique name, and click **Save**.

Note SRRG Label column can be edited only for assigned SRRGs.

Manage SRRG Assignments

A simple wizard enables you to select specific devices and links, see which SRRGs are assigned to them and change the assignments as required.

To manage SRRG assignments:

Step 1 In the left sidebar, select **Maps > Topology Maps > Network Topology**.

Step 2 Click on the Geographical Map toggle button in the top right corner of the map.

Step 3 Click the **Shared Risks (SRRGs)** button above the map and select **Manage Assignments**. The Manage SRRG Assignments wizard opens.

Step 4 Select the devices/links for which you want to manage SRRG assignments. You can either click on the required devices/links in the map or click in the box in Step 1 of the wizard and select devices from the list.

Step 5 Click **Next**. You will see a list of all the SRRGs common to all the devices/links you selected in the previous step. If an SRRG is assigned to one of the selected devices but not to the others, it will not be shown in the list. The SRRGs are color-coded based on whether they are the default on the device, assigned, or yet to be assigned. Click on the question mark icon to see the legend.

Step 6 Click the Plus icon and select additional SRRGs for the selected devices/links or create a new SRRG on the fly by typing an SRRG name. If the name is unique, a Create New link will appear. Click on the link to create the SRRG.

Step 7 If you created a new SRRG in the previous step, you can now choose a pool type and an SRRG resource pool of the selected type. The SRRG's ID will be taken from the range defined for the selected SRRG pool. The SRRG ID includes the bits for region and type in addition to the number within the range.

Step 8 Click **Next** to see a summary of your selections and SRRG assignments.

Step 9 Click **Finish**. You will be notified if the SRRG modification was successful. If it failed, an error dialog will provide details of the failure.

Create and Manage SRRG Pools Types and Resource Pools

Using SRRG pool types and resource pools, SRRGs can be grouped into categories for identification and ID allocation purposes. Each pool type has a range of SRRG IDs. You can create multiple SRRG resource pools of a specific pool type, each with a range of SRRG IDs that is within the range defined for the pool type. When you create a new SRRG for devices or links, you can assign it to a specific SRRG pool type and resource pool. The ID for the new SRRG will be created from the ID range of the selected resource pool.

Note Configlet Access permissions are required to manage SRRG pool types and pools.

To create SRRG pool types and resource pools, go to **Administration > System Settings > Inventory > SRRG Pool Types** or select **Pool Settings** from the SRRGs menu in the geo map.

To create a new SRRG pool:

Step 1 Go to **Administration > System Settings > Inventory > SRRG Pool Types** and check the existing pool types for the relevant pool type for your new SRRG pool. If it doesn't exist, create a new pool type as follows:

a) In the SRRG Pool Types window, click the Plus icon to add a row to the table.
b) In the Name field, enter a unique name for the pool type that represents the grouping you want to create for the SRRGs. For example, "NCS 2000 devices".
c) In the Type ID field, enter an ID from 0 to 14. Refer to the table of pool type definitions in About SRRG Pools and SRRG IDs, on page 217 for guidance as to the available range of IDs per pool type ID.
d) Enter a value for the start and end of the ID range for this pool type. You can use the full range or a subset of the available range. The tooltip on the Start Range or End Range field displays the available range for the pool type.
e) Click **Save**.

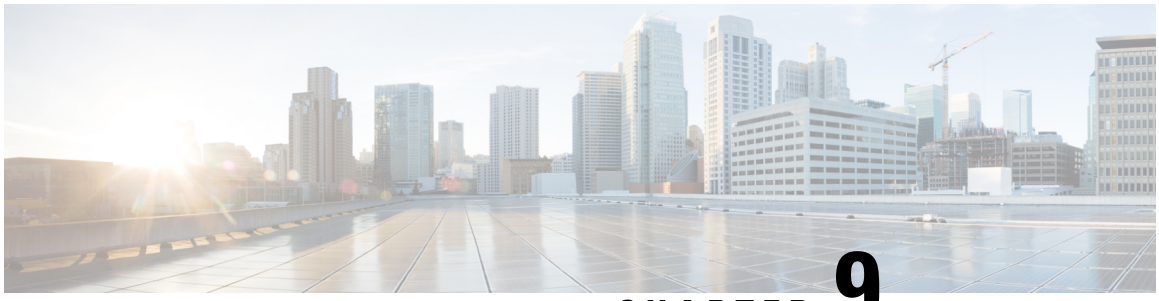
Step 2 Create the SRRG pool as follows:

a) Go to **Administration > System Settings > Inventory > SRRG Pool**.
b) In the SRRG Pool window, click the Plus icon to add a row to the table.
c) In the SRRG Pool Details area, select the required pool type from the Type dropdown menu.
d) Enter a unique name for the SRRG pool and optionally, a description.
e) From the Group dropdown menu, select a device group for this SRRG pool.
f) Enter the start and end of the range of SRRG IDs for this pool. The range must be within the selected pool type's range.
g) Click **Save**.

The new SRRG pool is added to the SRRG Pools table. It will also be available for selection when creating an SRRG ID for selected devices or links.

PART IV

Monitor the Network



CHAPTER 9

Monitor Device and Network Health and Performance

Monitor Device and Network Health and Performance

How Device Health and Performance Is Monitored: Monitoring Policies

Monitoring policies control how Cisco Evolved Programmable Network Manager monitors your network by controlling the following:

- What is monitored—The network and device attributes Cisco Evolved Programmable Network Manager monitors.
- How often it is monitored—The rate at which parameters are polled.
- When to indicate a problem—Acceptable values for the polled attributes.
- How to indicate a problem—Whether Cisco Evolved Programmable Network Manager should generate an alarm if a threshold is surpassed, and what the alarm severity should be.

Monitoring policies are important because apart from controlling what is monitored, they determine what data can be displayed in reports, dashboards, and other areas of Cisco Evolved Programmable Network Manager. Monitoring policies do not make any changes on devices.

Only device health monitoring (that is, the Device Health monitoring policy) is enabled by default. Interface Health monitoring is not enabled by default to protect system performance in large deployments. Note that the Device Health monitoring policy does not apply to the Cisco NCS 2000 and Cisco ONS families of devices. To monitor those device types, use the optical monitoring policies listed in Monitoring Policies Reference, on page 949.

These steps summarize how you can configure a monitoring policy.

1. Use a monitoring **policy type** as a template for your monitoring policy, and give the policy a name that is meaningful to you. Policy types are packaged with Cisco Evolved Programmable Network Manager and make it easy for you to start monitoring different technologies and services, such as Quality of Service, Optical SFP, and TDM/SONET. A complete list is provided in Monitoring Policies Reference, on page 949.

2. Adjust your policy's polling frequencies or disable polling altogether for specific parameters.
3. Specify the threshold crossing alarms (TCAs) you want Cisco Evolved Programmable Network Manager to generate if a parameter's threshold is surpassed. Some TCAs are configured by default; you can adjust or disable them, and configure new TCAs.
4. Specify the devices you want your policy to monitor. Devices are filtered depending on the policy type.
5. Activate your policy. The polled data is displayed in dashboards, reports, the Alarms and Events table, and other areas of the web GUI.

Monitoring policies collect data by polling network and device attributes at fixed polling intervals. The policy may run outisde of the polling interval due to:

1. Server load on account of processes like daily backup and daily inventory collection
2. Issues in connecting to the device or network latency
3. Collecting data from the device takes longer than the polling interval configured.

If there are devices being polled or in queue from a previous policy run, the policy skips polling these devices in the current polling interval. This behavior could result in a loss of up to 10 percent of monitored data for certain devices.

To view and administer monitoring policies, choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**.

Navigation	Description
Automonitoring	Lists the policies that are enabled by default in Cisco Evolved Programmable Network Manager. Only the Device Health monitoring policy is enabled by default. You can adjust the settings for this policy.
My Policies	The policy you create is listed here. When you choose a policy from **My Policies**, you can view the policy's details.

Set Up Basic Device Health Monitoring

The Device Health monitoring policy is enabled by default. It monitors both Cisco devices and third-party devices. For Cisco devices, the device health monitoring checks managed devices for CPU utilization, memory pool utilization, environment temperature, and device availability. For third party devices, the device health monitoring checks managed devices for device availability only. This policy also specifies thresholds for utilization and temperature which, if surpassed, trigger alarms that are displayed in the GUI client.

To view the current settings for this policy, choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then select **Automonitoring** from the list on the left. You can also adjust the polling frequency and threshold for the different parameters. To adjust a polling frequency or threshold, use the drop-down lists that are provided in the GUI client.

You might also want to create a device health monitoring policy that monitors specific devices—for example, devices of a certain type or in a certain geographical location. For instructions on how to do this, see Adjust What Is Being Monitored, on page 230.

Set Up Basic Interface Monitoring

Interfaces are not monitored by default. This protects the system performance for networks with a large numbers of interfaces.

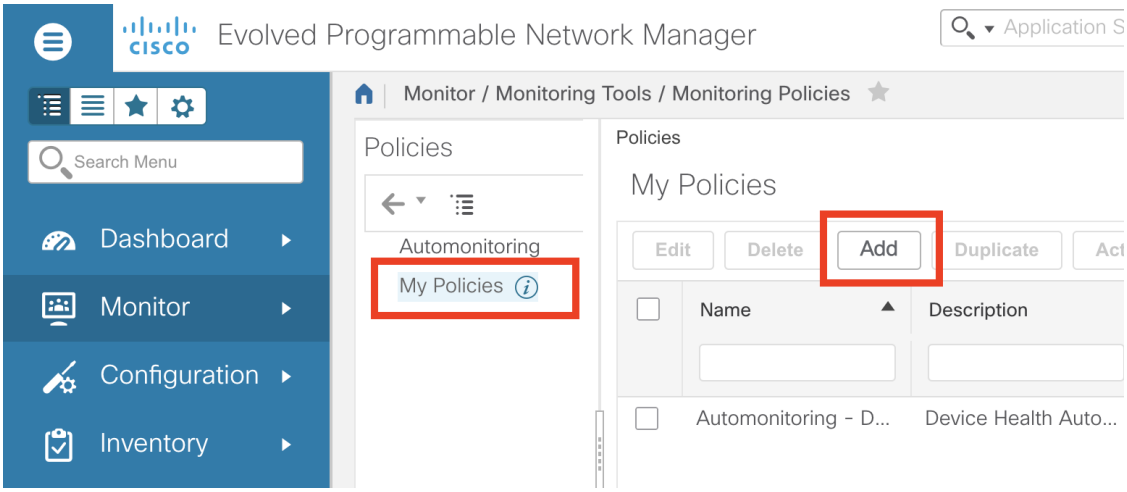
Use this procedure to set up basic interface monitoring.

To set up and enable interface monitoring:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then select **My Policies** in the list on the left.

Step 2 Click **Add** to create a new policy.

Figure 7: Add Monitoring Policies



Step 3 Choose **Interface Health** for generic interface monitoring. If you are monitoring optical devices, choose **Optical 15 Mins** or another optical policy (see Monitoring Policies Reference, on page 949).

When you select a policy, Cisco Evolved Programmable Network Manager populates the window with the policy settings.

Step 4 Enter the name and description.

Step 5 From the **Device Selection** drop-down list, click the appropriate radio button and select the device or device groups that you want to monitor. For the Interface Health monitoring policy, you can also select port groups.

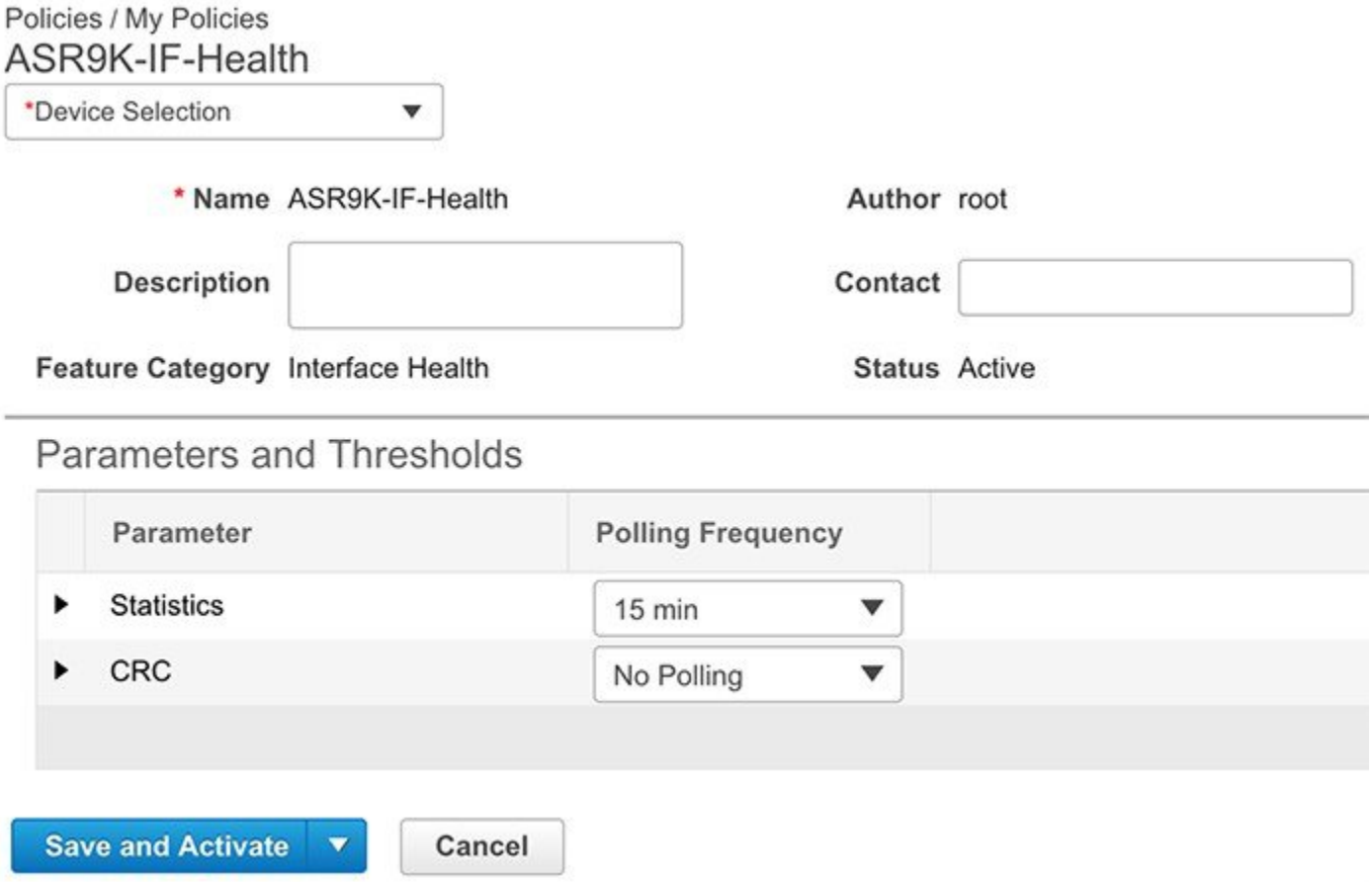
Cisco Evolved Programmable Network Manager only lists the devices or ports applicable to the policy that you selected in Step 3.

Note the following:

- If you want to use the default settings for polling and thresholds, proceed to Step 8.
- Due to a limitation in the current release of Cisco Evolved Programmable Network Manager, the Interface Health monitoring policy polls all the interfaces in your network for cyclic redundancy check (CRC) error data, not just the ones associated with the selected port group. Keep this in mind whenever you view CRC error data.

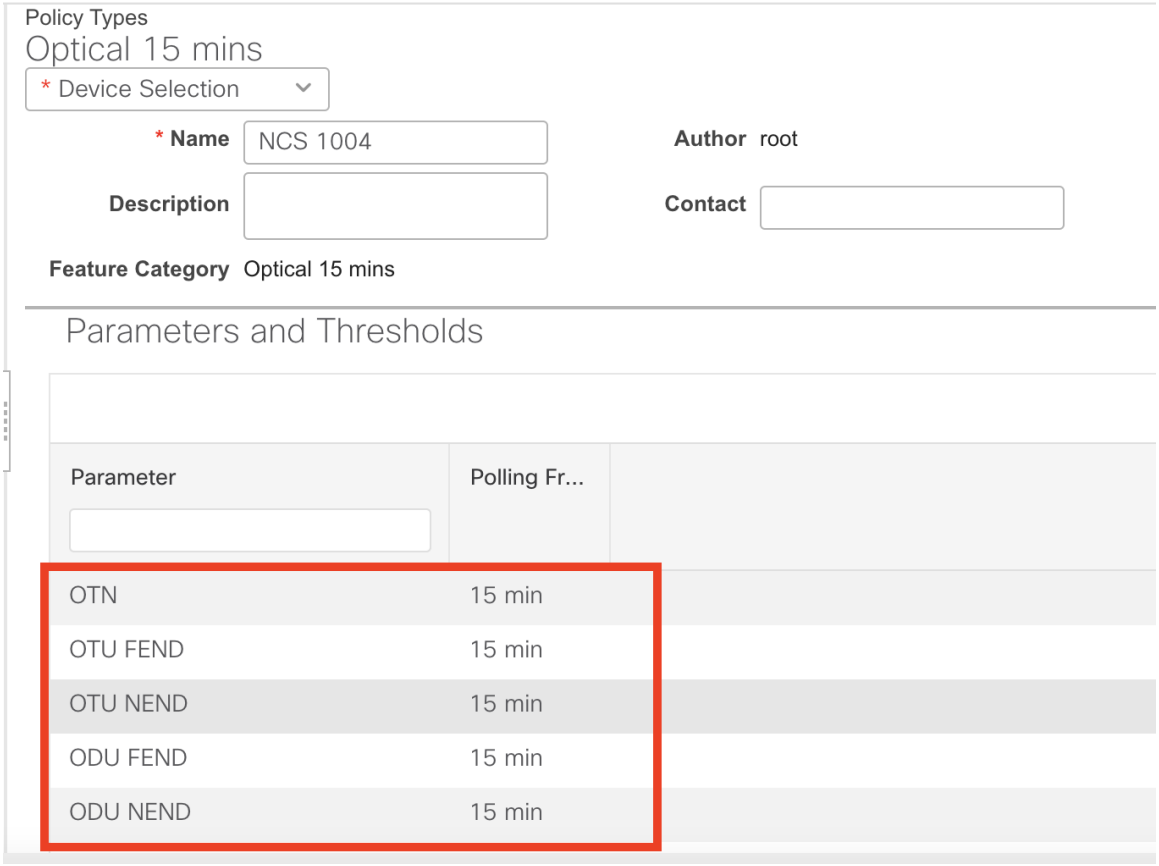
Step 6 To adjust how often the interface is polled, select a value from the **Polling Frequency** drop-down list. Some policies allow you to set polling frequencies for different parameters, while other policies have only one polling frequency that is applied to all the parameters.

For example, the following shows a policy that monitors Cisco ASR 9000 interfaces. It uses the **Interface Health** policy type, where all parameters are polled using the same interval.



Alternatively, the following shows a policy that monitors Cisco NCS 1004 interfaces.

It uses the **Optical 15 mins** policy type, where each interface type has its own polling interval. You can edit the interval by double-clicking it.



Step 7 If the policy supports TCA customization, you can adjust the thresholds. See Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 234.

Step 8 Click:

- **Save and Activate** to start monitoring immediately.
- **Save and Close** to save the policy and activate it later.

Use the Dashboards To Check Network and Device Health

Cisco Evolved Programmable Network Manager provides a variety of dashboards for monitoring your devices and network. The following are some examples of what dashboards can provide:

- Network-wide real-time status information, such as unreachable devices, interfaces that are down, and the most recent alarms.
- Summarized historical information, such as the most frequently-occurring alarms, and the devices and interfaces with the highest memory and CPU utilization.
- Device-specific information, such as a device's availability history, utilization, interface statistics, and alarms.

- Technology-specific information, such as Carrier Ethernet services.

For information on dashboards, see Set Up and Use the Dashboards, on page 4.

Check What Cisco Evolved Programmable Network Manager Is Monitoring

This topic explains how to get the following information:

- Which policies are activated, their status, and their history.
- The specific parameters that Cisco Evolved Programmable Network Manager is polling, the frequency at which they are polled, and their threshold crossing alarm (TCA) settings.
- Who created the policy and which policy type they used as its basis.

To find out what a policy polls, when the policy last ran, and whether the policy is currently active, choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then choose **My Policies**. Cisco Evolved Programmable Network Manager lists the monitoring policies you created or have access to, with the following information.

Policy Field	Description
Name	Policy name (specified by the policy creator). To find out who created a policy, see
Description	Policy description (specified by the policy creator).
Type	Template (policy type) used to create this policy. For information on the policy typ page 223.
Status	**Active** or **Inactive**.
Threshold	Whether the policy monitors parameter thresholds and generates TCAs. If **Yes** is d
Activation History	Active monitoring policy—Displays the number of times the policy was activated, • When the policy was activated. • Which devices were polled at each policy run. If the list is very long, hover yo Inactive monitoring policy—Displays **Not Available**.
Collection Status	Active monitoring policy—Provides a hyperlink to a Collection Status popup winc • The Device name, IP address, and availability state of each device that was po • Which parameters were polled at each policy run. If the list is very long, hover Inactive monitoring policy—Displays **Not Available**.

To view polling frequencies and TCA details, from **My Policies**, select a policy from the list on the left. Depending on the policy type, the following information is displayed.

Note To view the Optical 1 day, Optical 15 mins, and Optical 30 secs parameters, refer to the Monitoring Policies Reference, on page 949.

Policy Field	Description
General Information	Name, description, creator, status, policy type (Feature Category). For informati Policies, on page 223.
Device Selection	Devices which the policy is monitoring.
Polling Frequency	How often Cisco Evolved Programmable Network Manager polls the device pa
Parameters and Thresholds	Which parameters are polled and their TCA settings, if any. To view the TCA s the parameters polled by the various policy types, see Check Which Parameter

Check Which Parameters and Counters Are Polled By a Monitoring Policy

Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228 explains how to find out which monitoring policies are currently activated. To find out which *parameters* are being polled by a policy, follow this procedure.

Note To view the Optical 1 day, Optical 15 mins, and Optical 30 secs parameters, refer to the Monitoring Policies Reference, on page 949.

You can use this procedure to check:

- Parameters polled by existing policies (regardless of whether a policy is active or inactive).
- Parameters used by a policy type. This is useful if you want to check what a new policy will poll before creating the policy.

Step 1 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then choose **My Policies**. The web GUI lists the existing active and inactive monitoring policies.

Step 2 **To check the parameters used by an existing policy**:

- To view parameters that were polled most recently, locate the policy in the window on the right, then click **Details** in the **Collection Status** column. In the Collection Data dialog box, hover your mouse over the text in the **Parameter** column to list the polled parameters.
- To view the parameters along with their polling settings, expand **My Policies** in the navigation area on the left, then choose the policy you want to check. The window on the right displays the parameters and their polling settings.

Step 3 **To check the parameters used by a specific policy type**:

a) Click **Edit**. The supported policy types are listed in the navigation area on the left.
b) Choose a policy type. The window on the right displays the parameters polled by that policy, along with default polling and TCA settings. (These settings can be customized when a monitoring policy is created.)

Policies Pane Pop-Up Window

From the **Policies** pane in the **Monitoring Policies** page, you can open a pop-up window that provides summary information and action links for the corresponding policy or policy folder. To open a pop-up window, place your cursor over the appropriate *i* (**information**) icon.

- If you open the pop-up window for a policy, it displays information such as the policy's type, status, and timestamp for the last time it was updated. From the **Actions** area, you can click links to edit, delete, or duplicate the policy.
- If you open the pop-up window for a policy folder, it indicates the folder's name and the number of policies that belong to it. From the **Actions** area, you can click links to delete the folder or add a new sub-folder. Note that you can only add and delete folders within **My Policies**. Also, when user-created folders are in place, you need to specify the destination folder whenever you create a new policy.

Check a Monitoring Policy's Device, Polling, Threshold, and Alarm Settings

To check a monitoring policy's threshold and alarm settings:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then choose **My Policies**.

Step 2 Select the monitoring policy and click **Edit** to open the policy details.

Step 3 To find out which devices the policy is monitoring, click the **Device Selection** drop-down list. Devices that are monitored are indicated with a check mark. To add or remove devices, see Change the Device Set a Policy is Monitoring, on page 234.

Step 4 To find out the polling interval the policy is using, check the **Polling Interval** setting. For per-parameter polling, you must expand the individual parameters to see the setting. To adjust the polling settings, see Change the Polling for a Monitoring Policy, on page 234.

Optical policy polling frequencies cannot be changed; they can only be disabled.

Step 5 To find out the thresholds and alarm settings the policy is using, expand the parameter in the **Polling and Thresholds** area. To change the threshold and alarm settings, see Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 234.

Optical policy thresholds cannot be customized.

Adjust What Is Being Monitored

To make adjustments to what Cisco Evolved Programmable Network Manager is monitoring, use the guidance in the following table to find the best method for your needs.

If:		See:
Cisco Evolved Programmable Network Manager is collecting the data you need, and...	... you want to change the polling frequency	Change the Polling for a Monitoring Policy, on page 234
	... you want to adjust the alarm behavior	Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 234
	... you want to adjust which devices are monitored	Change the Device Set a Policy is Monitoring, on page 234
Cisco Evolved Programmable Network Manager is *not* collecting the data you need, and...	... a similar monitoring policy already exists	Create a New Monitoring Policy Based On An Existing Policy, on page 231
	... no similar monitoring policies exist, but one of the policy types contains the parameters you want to monitor	Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232
	... no similar monitoring policies exist, and none of the policy types contain the parameters you want to monitor	Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 232
	... you want it to monitor unsupported or third-party devices	

Create a New Monitoring Policy Based On An Existing Policy

Step 1 Check what is currently being monitored to verify that you need to create a new policy. See Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.

Step 2 Create the duplicate.

a) Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then click **My Policies** from the list on the left.
b) Locate the policy you want to duplicate.
c) Select the policy, then click **Duplicate**.
d) In the **Duplicate Policy Creation** dialog, choose the parent folder, enter a policy name and description, then click **OK**.

Step 3 Make your changes to the duplicate.

a) Locate the policy under **My Policies**.
b) Select the policy and click **Edit**.
c) Make your changes as needed. See:

- Change the Device Set a Policy is Monitoring, on page 234
- Change the Polling for a Monitoring Policy, on page 234
- Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 234

Step 4 Click:

- **Save and Activate** to save and activate the policy immediately on the selected devices. You can also choose to **Save and Deactivate** the policy.

Create a New Monitoring Policy Using Out-of-the-Box Policy Types

Step 1 Check what is currently being monitored. See Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.

Step 2 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then click **Add**.

Step 3 Select the policy type template you want to use from the **Policy Types** menu.

Step 4 Configure the new policy:

a) Select the devices, device groups, or port groups from the **Device Selection** drop-down list. (Not all monitoring types can be applied to port groups.)

b) Enter a name and contact, and edit the description.

c) Under **Parameters and Thresholds**, configure the polling settings, parameter values, and alarm conditions. See Change the Polling for a Monitoring Policy, on page 234 and Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 234.

Step 5 Click:

- **Save and Activate** to save and activate the policy immediately on the selected devices.
- **Save and Close** to save the policy and activate it at a later time.

Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices

You can design custom MIB polling policies to monitor third-party or Cisco devices and device groups. You can also create custom MIB policies to monitor device features, for which Cisco EPN Manager doesn't provide default policies. Using this feature, you can:

- Upload the SNMP MIB for the device type, then choose devices and attributes to poll and the polling frequency.
- Upload a single MIB definition file or a group of MIBs with their dependencies as a ZIP file.
- Display the results as a line chart or a table.

This feature allows you to easily repeat polling for the same devices and attributes and customize the way Cisco devices are polled using SNMP.

You can create a maximum of 25 custom MIB polling policies.

To create a custom MIB polling policies, follow these steps:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then choose **My Policies** and click **Add**.

Step 2 From the **Policy Types** menu, select **Custom MIB Polling**.

Step 3 Enter a name for the policy.

Step 4 Under the **MIB Selection** tab, specify the polling frequency and enter the MIB information.

- If Cisco EPN Manager does not list the MIB you want to monitor in the MIBs drop-down list, download the MIBs you want to monitor from the following URL: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2
- To upload a MIB, specify a filename extension only if you are uploading a ZIP file.
- If you are uploading a ZIP file, ensure that all dependent MIB files are either included in the ZIP or already present in the system.
- Ensure your upload file and the MIB definition have the same name. If you are uploading a ZIP file, you may name it as you please, but the MIB files that are packaged inside it must also follow the same convention (for example: MyMibs.zip is acceptable, as long as all MIB files in the ZIP match their MIB names).

Step 5 To test the policy that you created on a device before activating it, click the **Test** tab and select a device on which to test the new policy.

Step 6 Click **Save and Activate** to immediately activate the policy on the devices specified.

Schedule Custom MIB reports

You can schedule reports to monitor the custom MIB polling policies. This feature enables you to generate reports at intervals for custom MIBs:

To schedule a custom MIB report, follow the steps given below:

Before you begin

Before scheduling a custom MIB report, create a custom MIB polling policy as given in Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 232.

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard** > **User Jobs**, and choose **Custom MIB Report Jobs**.

Step 2 Click **+** icon to open **Add Custom MIB Report Job** window.

Step 3 Enter the Report Name and select the Policy Name.

Step 4 In the **Schedule Settings** section, select the Start Time and Recurrence intervals for the custom MIB report.

Step 5 Click **Save** to schedule a custom MIB report.

Step 6 To view the scheduled report and export the data, click the report name (hyperlink), which opens a window with all the reports generated at given intervals. You can click the **Generated report can be downloaded here** option to export the report data in CSV format. For more information on reports, see Reports Overview, on page 281.

Check the Status of Past Monitoring Policy Data Collections

To check a monitoring policy's past data collection:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then click **My Policies**.

Step 2 Locate the policy, and under the **Collection Status**, click **Details** to open the Collection Data dialog. To see which parameters were polled for a device, hover your mouse over the text in the Parameter column.

Change the Device Set a Policy is Monitoring

You can customize how often monitoring information is gathered (polling interval). Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1 Choose **Monitor > Monitoring Policies > My Policies** and select the policy you want to edit.

Step 2 Check the policy you want to edit and click **Edit**.

Step 3 Click the Device Selection drop-down list.

Step 4 Select and deselect devices as needed.

Step 5 Click **Save and Activate** to save and activate the policy immediately on the selected devices.

Change the Polling for a Monitoring Policy

You can customize how often monitoring information is gathered (polling interval). Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then click **My Policies**.

Step 2 Select the policy you want to edit and click **Edit**.

Step 3 Adjust the polling frequency. How to adjust polling depends on the monitoring policy type.

- Policies with one polling frequency that applies to all attributes—To adjust the polling frequency, select the new interval from the Polling Frequency drop-down list. To disable polling, deactivate the policy by clicking **Save and Deactivate** at the bottom of the page.
- Policies with per-attribute polling frequencies—To change the polling setting for a specific attribute, double-click the attribute line and change the setting. Choosing **No Polling** will disable polling for that attribute only.

To disable polling for all attributes in the policy, deactivate the policy by clicking **Save and Deactivate** at the bottom of the page. Do not proceed to the next step.

Step 4 Click **Save and Activate** to save and activate the policy immediately on the selected devices.

Change Thresholds and Alarm Behavior for a Monitoring Policy

You can customize the threshold value that indicates a problem and whether Cisco Evolved Programmable Network Manager should generate an informational event or an alarm (of any severity) when a problem is

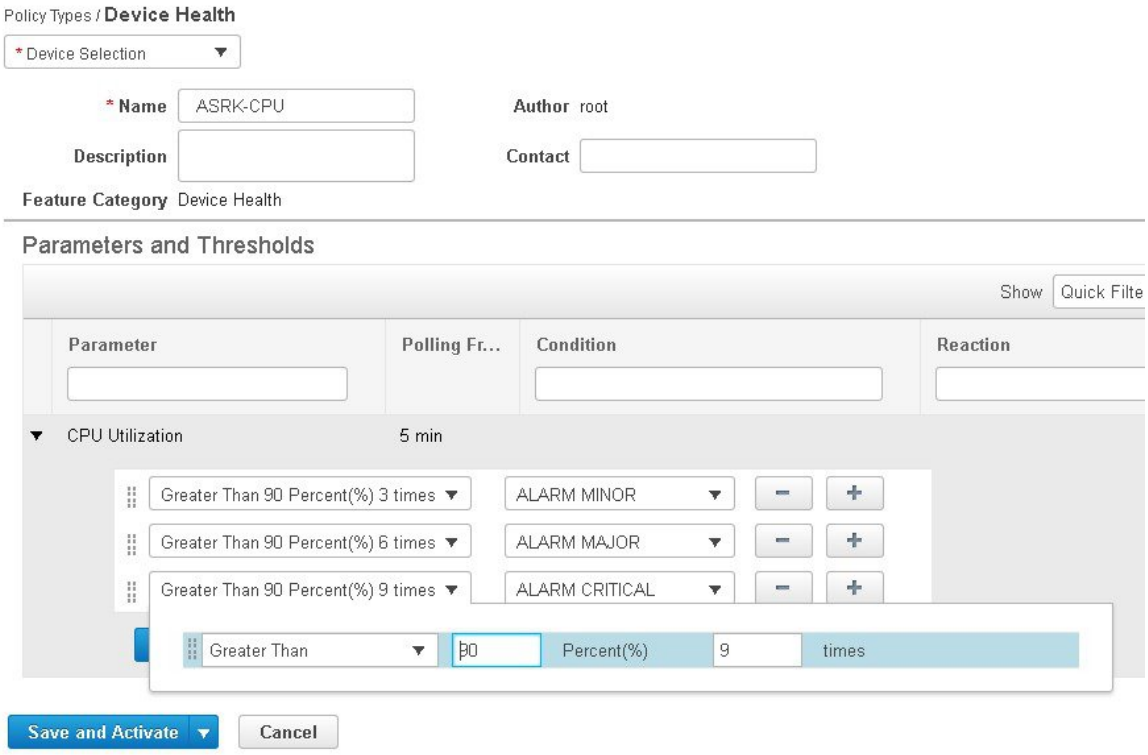
detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then choose **My Policies**.

Step 2 Select the policy you want to edit and click **Edit**.

Step 3 Locate the parameter you want to change. You can search for the parameter by entering a string in the **Parameter** text box.

Step 4 Expand the parameter. You can change an existing condition or add new conditions, as in the following figure, which specifies thresholds and alarms for CPU utilization on Cisco ASR 9000 devices.



Note You can have only total of 50 thresholds for each metrics as given in the below tables.

Step 5 When you are done, click **Save and Activate** to save and activate the policy immediately on the selected devices.

Run Performance Tests

When you run a performance test, Cisco Evolved Programmable Network Manager connects to the network devices in real time to retrieve the information. Reports, on the other hand, use historical data that is saved in the database. See these topics for more information, depending upon the type of test you want to run:

- Performance Test Based on Y.1564 for EVCs, on page 667
- Performance Test Based on Y1731 for EVCs, on page 670

- Performance Test for Optical Circuits, on page 671
- Performance Test for Circuit Emulation Services, on page 673

Cisco Evolved Programmable Network Manager also supports running OTDR performance tests on OTS optical links. For more information, see Run an OTDR Performance Test on an OTS Link, on page 236.

Run an OTDR Performance Test on an OTS Link

An Optical Time Domain Reflectometer (OTDR) test is a graphical signature of a fiber's attenuation along its length which provides insight into the performance of the link components (cable, connectors and splices). It allows remote diagnosis of OTS link related issues (such as degraded devices, splices and bends in the cables).

The OTDR test can be initiated only on OTS links that are connected to the OTDR port in the TNC card.

Note For NCS1001 devices, an .xml file with the device specific configuration needs to be added under /opt/CSCOlumos/conf/ncs1k-otdr-ports.xml in case the default xml configuration is varying with the device configuration. Doing so, provides an association/connection between the OTS link associated EDFA line port and the OTDR port.

Some of the OTDR functions are limited to specific user groups, as described in the table below:

User Group		Can view OTDR scan results?	Can run and analyze OTDR scan?	Can configure OTDR scan?	Can set baseline?
Web GUI	Root	Yes	Yes	Yes	Yes
	Super Users	Yes	Yes	Yes	Yes
	Admin	Yes	Yes	Yes	Yes
	Config Managers	Yes	Yes	Yes	Yes
	System Monitoring	Yes	Yes	No	Yes

The OTDR scan can be accessed from the **Actions** menu in the Links tables or from the Interface 360 view. The OTDR Scan menu option is only available for links or interfaces on which OTDR is supported.

To run an OTDR scan:

Step 1 Access the OTDR scan window in one of the following ways:

- Choose **Inventory** > **Other** > **Links**. Select the required OTS link, then choose **Actions > OTDR Scan**.
- Open the Interface 360 view for one of the sides of the link you want to test and choose **Actions > OTDR Scan**.

The OTDR Scan window opens and displays the results of the last scan for this link.

Step 2 In the Configure tab, check the OTDR configuration settings on both sides of the link and modify them if necessary. See Configure OTDR Port Values, on page 238.

Step 3 In the Scans tab, click the arrow next to **Change Scan Direction** to view the direction settings. In the **Scan Direction** area, the A-side and Z-side of the selected OTS link are represented and you can select the direction in which you want to run the test.

Step 4 Under **Scan Direction**, select the direction of the test by clicking on the relevant arrow. Note that above each direction arrow is information indicating when the last scan for that direction was run or if there are new scans to download.

The table displays all system, Baseline & imported scans for the selected direction. You can:

- Click the *i* icon to view one or multiple scans if available.
- Click the mug icon to download a scan.

  Note TFTP must be enabled to see/download the scan result from device to Cisco EPN Manager.

- Select one or multiple scans and click the round arrow to download these scans.
- Filter and sort data in the columns.

Step 5 Start a new scan in one of the following ways:

- Select a specific scan from the table and then click the **Start Scan** button.
- Click **Start Scan** to start a scan without selecting a specific scan from the table. The **Start New Scan** dialog appears. Select **Distance Profile** and **Scan mode** as required and click **Continue** to start the scan.

You can view the progress of the scan in the **Change Scan Direction** window. To stop a scan that is in progress, click the **Cancel** link above the direction arrow in which the scan runs.

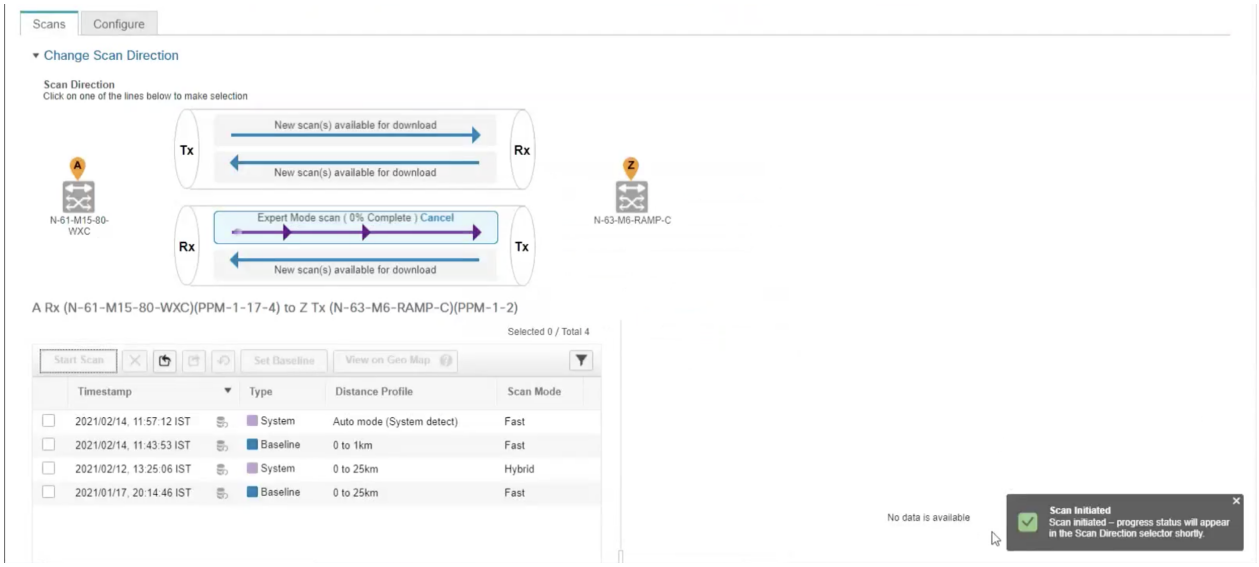
Step 6 Once the scan is complete,

- A graphical representation of the scan result is displayed with the power readings (dB) over a specified distance profile (km). You can also view the baseline graph to compare with the last scan reading.
- If you click the *i* icon, the **Events** table displays a table with the distance (km), baseline reading (dB) and previous scan reading (dB). They display the relative/absolute threshold, which is the comparison of the baseline to the scan results. Use the Type field to filter Reflection, Insertion Loss, or Reflection with Loss type of event detail. You can analyze an event by selecting the event in the table and clicking **Analyze Event**. This causes the scan to be re-run with the specific location of the event.

  Note
  - An alarm is raised if the threshold exceeds the value set on the device. The Reflection, Insertion Loss and Reflection with Loss information is represented with an icon in the **Type** field.
  - Recurrence and threshold values are not supported for NCS1001 devices.
  - For NCS2K devices, when you start a new scan you can select between **Fast**, and **Hybrid** scans. This option is not available for NCS1001 devices.

- Click **View on Geo Map** to see the scan results within the context of the geo map. See View OTDR Scan Results in the Geo Map, on page 241

Figure 8: View Scan Event Details



Step 7 (Optional) Click **Set Baseline** to set an OTDR test baseline. Setting a baseline helps you to compare with the last scan results.

Set Baseline is not supported for NCS1001 devices.

Step 8 To export the scan results, see Export the OTDR Scan Results, on page 240.

Step 9 To import the scans, see Import OTDR Scan, on page 240.

Step 10 To schedule the OTDR scan to be run at predefined regular intervals, see Provision OTDR Scan Recurrence, on page 240.

Configure OTDR Port Values

For the OTDR scan, you can either use the default settings for the TNCS cards for each sector or you can modify the settings as required.

Step 1 Access the OTDR scan page as described in the Run an OTDR Performance Test on an OTS Link, on page 236 topic.

Step 2 In the **Configure** tab, select a device from the **Device** drop-down list. A table is displayed listing all the sectors with the default values for the following columns:

- Scan Status—Cumulative status of the scans
- Loss Sensitivity (dB)
- Reflection Sensitivity (dB)
- Start Point (km)
- End Point (km)
- Pulse Width (microseconds)
- Resolution (m)

- Measure Time (s)
- Baseline—Baseline is not set by default
- Threshold Loss (dB)
- Threshold Reflection (dB)
- Recurrence—Recurrence is not set by default

The OTDR measurement ranges are categorized based on the fiber spans defined for each sector. Following are the OTDR measurement sectors:

- **Zone #1**—Distance 0 to 1 km
- **Zone #2**—Distance 0 to 25 km
- **Zone #3**—Distance 0 to 80 km
- **Zone #4**—Full distance
- **Expert Mode**—For custom distance settings, you can edit the start point and end point parameters
- **Auto Mode (System Detect)**—The end point parameter is defined automatically

Note For NCS1K devices only **Expert Mode** and **Auto Mode (System Detect)** is supported.

The distance profiles parameters listed in the **Configure** tab are refreshed for every 30 seconds.

If you enable **Enable Absolute Threshold** on the OTDR settings page, the baseline of OTDR algorithm will be disabled and the configured values (Absolute Event Loss Threshold (dB) and Absolute Event Reflection Threshold (dB)) in OTDR settings will be considered. You can configure the actual values which are configured under each sector.

When the **Enable Absolute Threshold** is disabled, the baseline algorithm will be active and correct alarm thresholds can be retrieved for the particular sector (zone#1, zone#2, and so on) not the Absolute Threshold values.

Step 3 To modify the OTDR settings on the device, click the **Device OTDR Settings** hyperlink. For more details on the OTDR settings, see the 'Configuring OTDR Auto Scan' section in Provision Optical Interfaces , on page 360.

Step 4 To edit the sector parameters, select the required Distance Profile in the table, and click **Edit**. A popup window is displayed.

Step 5 In the popup window:

- For **Zone #1** to **Zone #4**—You can edit Loss Sensitivity (dB) and Reflection Sensitivity (dB), Threshold Loss (dB), Threshold Reflection (dB), and Recurrence values. For information on setting the scan recurrence, see Provision OTDR Scan Recurrence, on page 240.
- For **Expert Mode**—You can edit all the columns in the table, except scan status and baseline.
- For **Auto Mode**—You can edit Loss Sensitivity (dB) and Reflection Sensitivity (dB), Threshold Loss (dB), Threshold Reflection (dB), and Recurrence values. The End Point value (length of the fiber span for OTDR scan) is defined automatically. The other values for the scan (Pulse Width, Measure Time, and Resolution) are then configured based on the detected length of the fiber span.

To enable absolute threshold, you need to select Absolute Fiber Pass Fail Criteria check-box in the **OTDR Settings** page.

Step 6 Click **Save**.

Provision OTDR Scan Recurrence

Follow the below procedure to set up OTDR scan recurrence on the selected ports:

Step 1 In the **Configure** tab of the OTDR Scan page, from the **Device** drop-down list, select the port on which you want to provision a recurring scan.

Step 2 Select the appropriate distance profile, and click **Edit.** A popup window is displayed.

Step 3 In the **Recurrence** area, set the scan frequency by choosing one of the following:

- None—No recurrence is set (default).
- Weekly—To schedule a weekly recurring scan, go to Step 4, on page 240.
- Intervals—To schedule a granular recurring scan, go to Step 5, on page 240.

Step 4 Select the desired day from the **on** drop-down list and enter the hours and minutes.

Step 5 Select the desired day range between 0 to 365 and enter the hours and minutes.

Step 6 Click **Save**.

Export the OTDR Scan Results

You can export the scan results to your local.

Step 1 Select the scan for which you want to create an export file.

Step 2 Click Export Scans icon.

The exported file (.sor format) will be downloaded to your local machine.

Import OTDR Scan

You can import the scan results from your local.

Step 1 Click the Import Scans icon.

The **Import Scan (.sor)** window appears.

Step 2 Click on **Browse** and select the .sor file which you require to import.

Step 3 Select a **Distance Profile** from the drop down list.

Step 4 Select the **Scan Direction** by clicking on the desired line which shows the direction.

Step 5 Click **Import**.

View OTDR Scan Results in the Geo Map

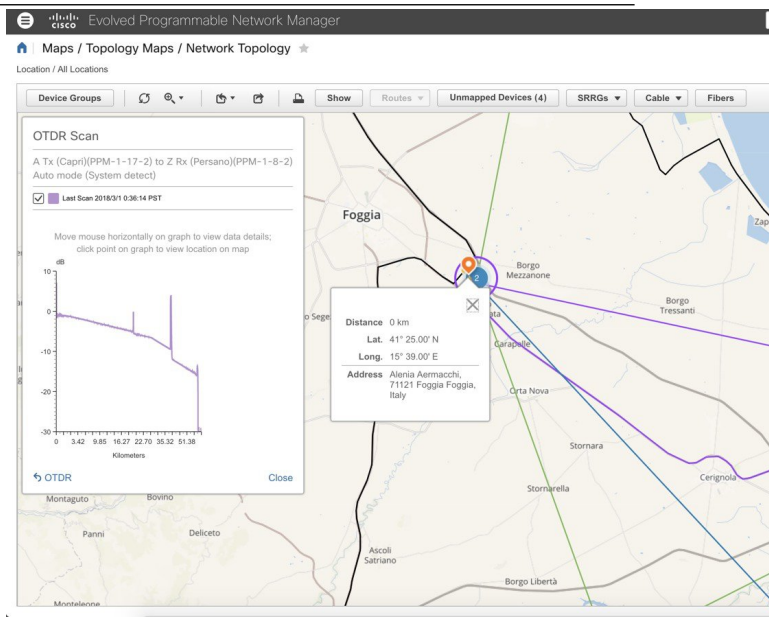
You can view the OTDR scan results in the context of the geo map in order to pinpoint the location of the fiber issues. For example, if the OTDR test reports a concentrated loss 20 km from the link endpoint, you can visualize on the map where this is geographically located.

Prerequisites:

- KML file containing fiber data and coordinates must be imported so that the fibers are visible on the geo map. See Import Location Data from a KML File, on page 213.
- The OTS link on which the OTDR scan is run must be associated with a fiber. See Associate Links to Fibers, on page 212.
- The A- and Z-side devices must be mapped on the geo map. See Place Unmapped Devices on the Geo Map, on page 206.

Procedure

	Command or Action	Purpose
Step 1	Launch the OTDR scan.	
Step 2	Define the scan parameters and run the scan.	
Step 3	Click **View on Geo Map**.	The geo map opens. The OTDR scan results graph is displayed on the left. The geo map zooms to show the relevant devices, link and fiber (highlighted in purple).
Step 4	Click on a point in the OTDR scan results graph.	A location icon appears on the exact location on the fiber on the geo map and a popup panel provides information about that location, including the distance in kilometers along the fiber, the exact coordinates, and the physical address. **Note** If the exact location cannot be calculated, the location icon shows an approximate location that is within a certain radius of the exact location. The radius (in km) is shown in the popup panel and a circle around the location icon in the map indicates that this is an approximate location within a radius of the exact location.

	Command or Action	Purpose
		
Step 5	If necessary, click on the **OTDR** link below the OTDR scan results graph to return to the OTDR scan page.	

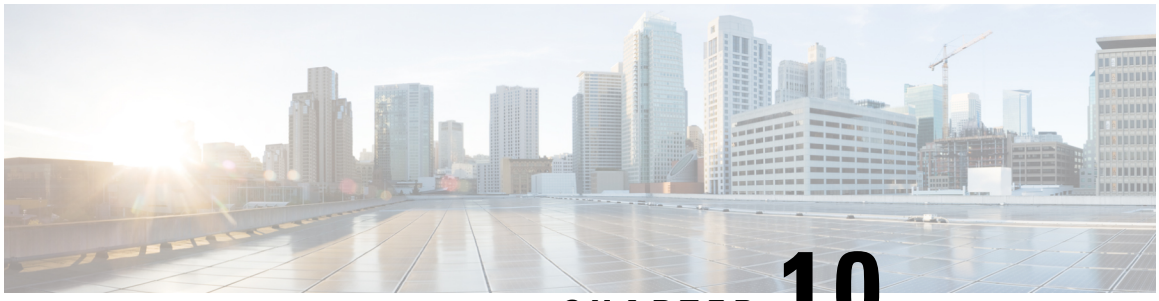
Monitor Network Performance Using Reports

Cisco Evolved Programmable Network Manager provides various reports to help you monitor your network's performance. The following are some examples:

- Environmental temperature, CPU, and memory utilization
- Interface errors and discards
- For Carrier Ethernet devices—IPSLA Ethernet OAM, PWE3, QoS, and other CE reports
- For Optical devices—Ethernet, OTN, SDH/SONET, and other optical reports

When you run a performance report, retrieves historical data that has been saved in the database. Reports can only display data that Cisco Evolved Programmable Network Manager has been configured to collect—in other words, data that are collected and monitored using monitoring policies. (No monitoring policies have to be enabled for event and alarm-related reports; that data is collected automatically.) For information on which monitoring policies must be enabled for the different reports, see Available Reports, on page 282.

Note Sometimes, while generating the report, the last sample may get omitted. This happens when the sample is inserted into DB after the report generation time. To avoid this, define an offset for any report by editing the file: **`/opt/CSCOlumos/conf/ReportExportSettings.properties`**



CHAPTER 10

Monitor Alarms and Events

What Are Alarms and Events?

An *event* is a distinct incident that occurs at a specific point in time, such as a port status change, or a device becoming unreachable. Events can indicate an errors, failures, or exceptional conditions in the network. Events can also indicate the *clearing* of those errors, failures, or conditions. Event have associated severities (which you can adjust as described in Change Alarm Severity Levels, on page 853).

An *alarm* is a Cisco Evolved Programmable Network Manager response to one or more related events. Only certain events generate alarms. Alarms have a state (cleared or not cleared) and a severity (Critical, Major, Minor, and so forth). An alarm inherits the severity of its most recent event. Alarms remain open until a clearing event is generated (or if the alarm is manually cleared).

Related Topics

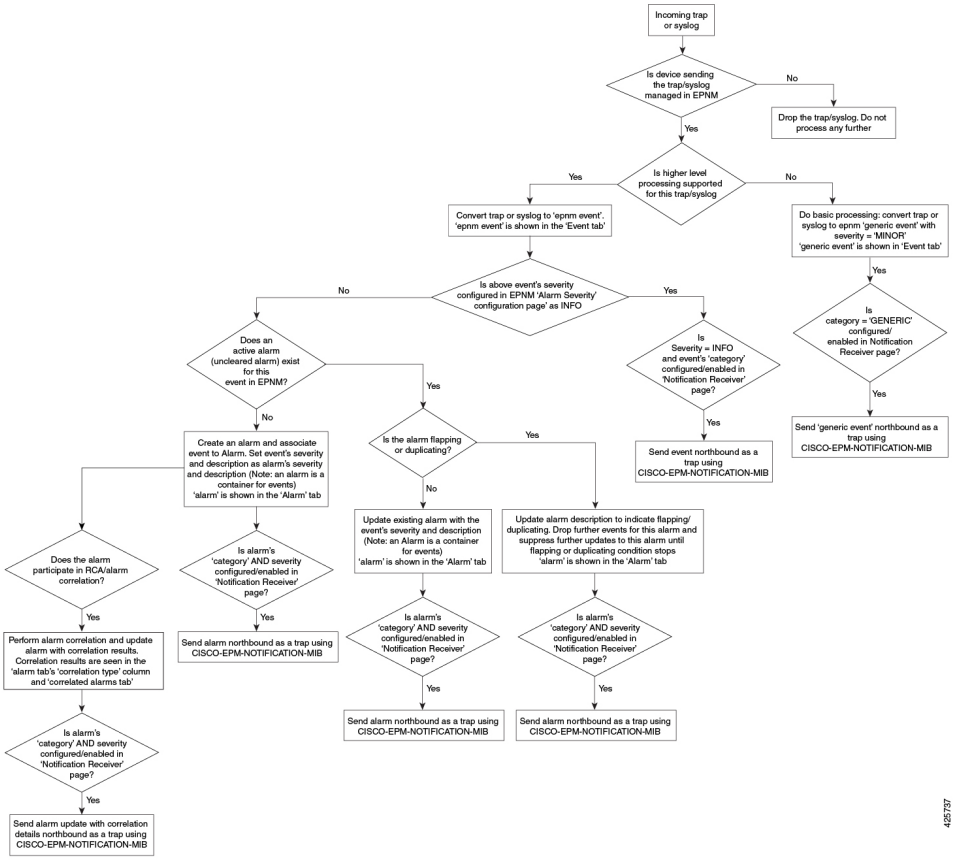
How are Alarms and Events Created and Updated?, on page 244

Acknowledge and Clear Alarms, on page 260
Interpret Event and Alarm Badges and Colors, on page 251

How are Alarms and Events Created and Updated?

The Cisco Evolved Programmable Network Manager processes SNMP traps, syslogs, and TL1 messages from both IPv4 and IPv6 devices. It maintains an event catalog that determines how it should respond to these events. The flowchart below represents the manner in which these alarms and events are processed:

Figure 9: Alarm processing flowchart



Cisco Evolved Programmable Network Manager performs the following general steps when it processes an event:

1. Checks the event catalog to see if higher level processing is necessary (as opposed to just generic processing) for the incoming SNMP trap, syslog, or TL1 message (by examining the raw event for predefined patterns).
    - If it cannot match the raw event to the catalog, the event is considered a *generic* event and it undergoes generic processing. Generic events are displayed events in the GUI and can be forwarded in notifications. (Generic event handling can be disabled; see Disable and Enable Generic Trap and Syslog Handling, on page 859). This is done so that none of the traps and syslogs received by Cisco Evolved Programmable Network Manager is discarded i.e., they either go through generic processing to create generic events or higher level processing to create alarms/processed events.

- If it can match the raw event to the catalog, the raw event is considered for higher level processing and Cisco Evolved Programmable Network Manager creates a processed event with a severity and potentially an alarm.

2. Identifies the device and device component that is causing the event (localizes the event).
3. Checks whether the supported event triggers inventory collection.

   Some events have specific rules that instruct Cisco Evolved Programmable Network Manager what information it should collect. For more information, see How Is Inventory Collected?, on page 52
4. Checks whether the event severity is INFO or CLEARED.
   - If it is INFO or CLEARED, Cisco Evolved Programmable Network Manager saves the event and displays it in the GUI.
   - If it is any other severity, Cisco Evolved Programmable Network Manager evaluates whether a new alarm should be opened (next step).
5. Checks whether an alarm already exists or a new alarm should be created.
   - If an alarm does exist, Cisco Evolved Programmable Network Manager associates the event to the existing alarm. The alarm severity is changed to match the severity of the new event, and the alarm time stamp is updated. If it is a clearing event (for example, a link up event), the alarm will be cleared.

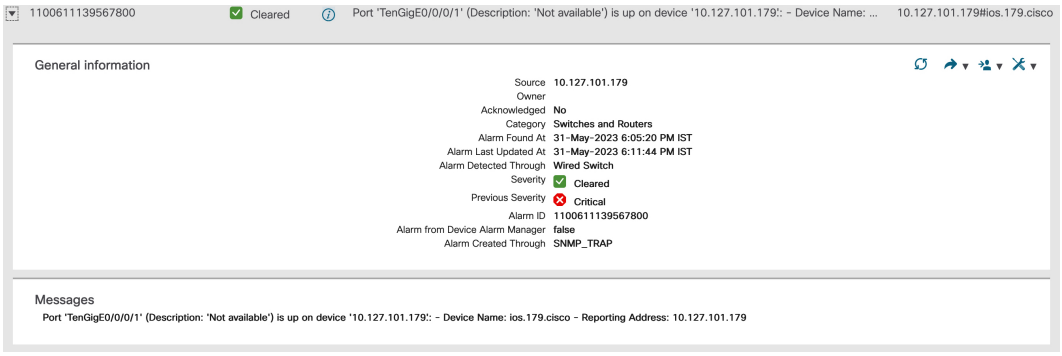
Note In some cases, a device may not generate a clearing alarm. The administrator should set the alarm auto-clearing interval as described in Change Alarm Auto-Clear Intervals, on page 854.

   - If an alarm does not exist, Cisco Evolved Programmable Network Manager creates a new alarm and assigns it the same severity as the event.
6. Checks whether the new or existing alarm can be correlated to any other alarms. (Note that here, alarms are being correlated with other alarms, not with events.) If they can be correlated, Cisco Evolved Programmable Network Manager does the following:
   - Identifies the causing alarm as the **root cause alarm**.
   - Identifies the resulting alarm as a **symptom alarm**.

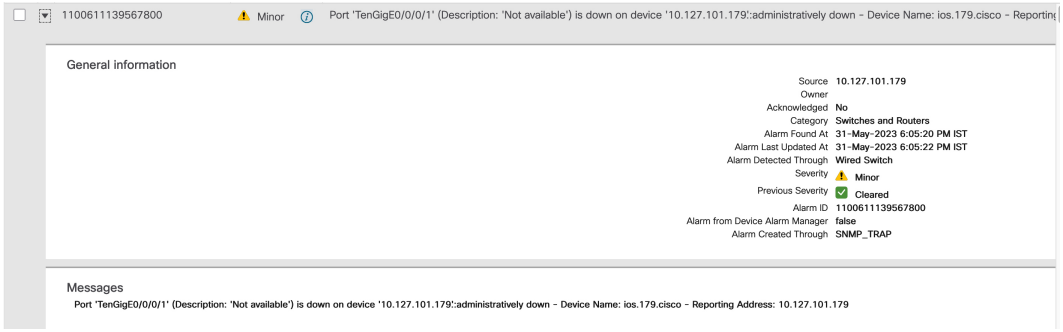
   You can identify uncleared correlated alarms by checking the Correlated Alarms tab in the Alarms and Events table. For more information on these kinds of alarms, see View Root Cause and Correlated Alarms, on page 256.

Example: Link Down Alarm

In this example, Cisco EPN Manager receives a Link Down trap that it receives from a device. Cisco EPN Manager generates a Link Down event and, because the port is operationally down, it also generates a Link Down alarm.



When Cisco EPN Manager receives a Link Up trap from the device, it generates a Link Up event and clears the alarm.



When a port is down for maintenance or has been disabled by a network administrator, Cisco EPN Manager raises a Link Down alarm with severity MINOR.

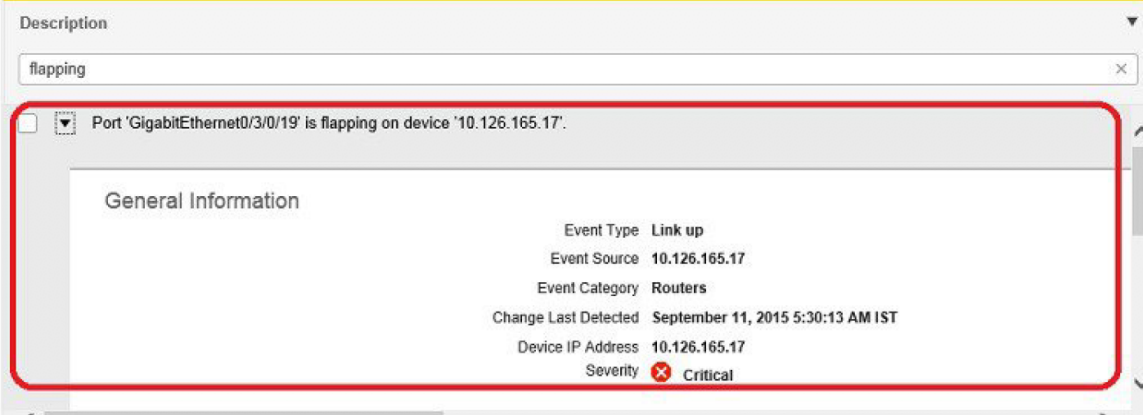
Note Severity of the Link Down alarms cannot be modified.

Flapping Events and Flow Controllers

Flapping is a flood of consecutive event notifications related to the same alarm. It can occur when a fault causes repeated event notifications (for example, a cable with a loosely fitting connector.) An event is identified as a flapping event if multiple events are of the same type, are associated with the same source, and recur in a short period of time. Cisco Evolved Programmable Network Manager will generate an alarm for flapping events. This alarm is generated when there are five occurrences of the same event within 300 seconds. The five occurrences could be of a sequence such as, Interface Down, Interface Up, Interface Down, Interface Up, Interface Down, and so on.

When an alarm is generated for a flapping event, the devices often go into a continuous synchronization state. This can prevent deployment of device configuration such as service provisioning, OAM, etc, on the device. However, in Cisco EPN Manager, when a monitored device raises a Flapping alarm, Cisco EPN Manager detects this alarm and stops further updates of the alarm until the flapping condition on the device is cleared.

The alarm detected as a Flapping Event is cleared based on an exit condition, which is that when there is no occurrence of the same event within the next 300 seconds, the alarm is cleared. This helps control the flow of events to avoid unnecessary triggering of device synchronization.



Which Events Are Supported?

Refer to the following documents for information on the events that are supported by Cisco Evolved Programmable Network Manager.

- Cisco Evolved Programmable Network Manager Supported Traps
- Cisco Evolved Programmable Network Manager Supported Syslogs
- Cisco Evolved Programmable Network Manager Supported TL1 Messages

For information about how unsupported events are handled, see View Events (Including Generic Events), on page 263.

Set Alarm and Event Management Preferences

- Set Up Your Alarm and Event Display Preferences, on page 247
- Customize the Alarm Summary, on page 250

Note Advanced users can also use the Cisco Evolved Programmable Network Manager Representational State Transfer (REST) API to access device fault information. For information on the API, click ⚙ at the top right of the Cisco Evolved Programmable Network Manager window and choose **Help** > **API Help**.

Set Up Your Alarm and Event Display Preferences

In the Alarms and Events tables, Cisco Evolved Programmable Network Manager displays the last 4000 alarms or events, by default. Cisco Evolved Programmable Network Manager can only display what is available in the cache (which may be less than 4000). If you want to see more than 4000 alarms or events, click **Show Alarm History** above the table.

Note The list of 4000 alarms and events also includes cleared alarms which are not displayed. Click **Show Alarm History** to see all the open alarms.

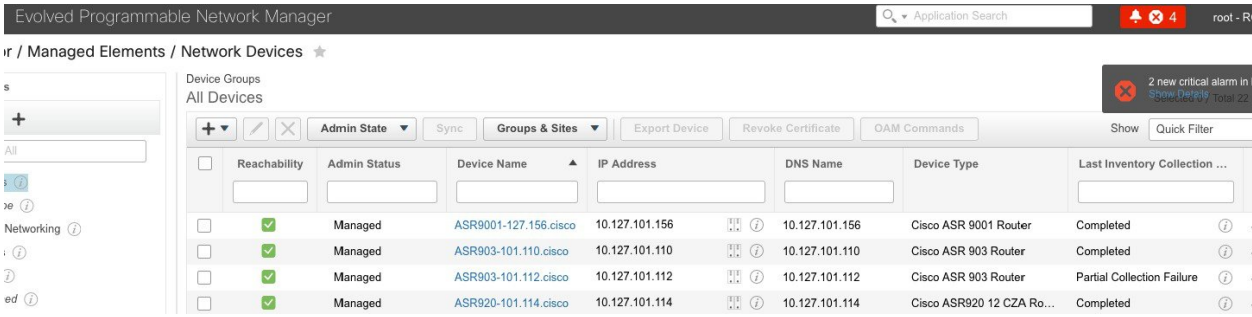
You can customize the following alarm and event display by clicking ⚙ at the top right of the Cisco Evolved Programmable Network Manager window and choosing **My Preferences**. After you make your changes, click **Save** to apply your new settings. Other settings, such as whether acknowledged, cleared, and assigned alarms are displayed, are controlled globally by the administrator. (see Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms, on page 850).

User Preference Setting	Description
Automatically refresh Alarms & Events page	Enables or disables automatically refreshing of the Alarms and Events page. If enabled, the page is refreshed according to the setting in **Refresh Alarm count in the Alarm Summary**.
Refresh Alarm count in the Alarm Summary every ___ minutes/seconds	Sets the refresh interval for the alarm count in the Alarm Summary (1 minute by default) (see Customize the Alarm Summary, on page 250).
Enable Alarm Badging on Alarms & Events page	When user enables Alarm Badging, alarm severity icons are displayed next to the device groups on the **Monitor** > **Monitoring Tools** > **Alarms & Events** page.
Disable Alarm Acknowledge Warning Message	**Note** This setting is only configurable if **Hide Acknowledged Alarms** is also enabled; that setting is disabled by default (see the previous table). Disables the following message from displaying when user selects an alarm and chooses **Change Status** > **Acknowledge**: **Warning: This alarm will not be generated, if the original event recurs again, within next 7 days, as it is acknowledged now. Clearing the alarm instead of acknowledging will cause the alarm to be generated if the event recurs again. Proceed with alarm acknowledgment?**
Disable confirmation prompt for "Clear all of this condition"	Disables the following message from displaying when user selects an alarm and chooses **Change Status** > **Clear all of this condition**: **Are you sure you want to clear all alarms of this condition?** (Disabled by default)

User Preference Setting	Description
Disable "Set severity to information" prompt for "Clear all of this condition"	Disables the following message which is displayed when user selects an alarm and chooses **Change Status** > **Clear all of this condition**: **Do you want to set the severity for the selected alarm's condition to Information?** **WARNING: This is a system-wide change that will prevent creation of future alarms of this condition. You can undo this change on the Severity Configuration page under System Settings.** (Disabled by default) **Note** Users with sufficient privileges can reset the severity to its original value using the procedure in Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms, on page 850.
Select alarm categories for Alarm Summary Toolbar	Controls what is displayed in the Alarm Summary (see Customize the Alarm Summary, on page 250).
When clearing all alarms of a condition, always set the condition's severity to Information	When user selects and alarm and chooses **Change Status** > **Clear all of this condition**. (Disabled by default)
Enable New Critical Alarm Count Notifications	Enables the notification pop-up that displays the count of critical alarms.The count gets updated once the alarm interval is refreshed depending on the interval set in **Refresh Alarm count in the Alarm Summary** (see Customize the Alarm Summary, on page 250). Only the outstanding critical alarms are displayed.

View Critical Alarm Notifications

The count of the critical alarms in the network is displayed as a notification pop-up in every page. The count gets refreshed every 1 minute or some interval depending on the interval set in the **My Preferences** page.



Click the **Show Details** hyperlink to view the list of critical alarms in the **Monitor** > **Monitoring Tools** > **Alarms and Events** > **Alarms** page.

Note Only the outstanding critical alarms are taken count and displayed.

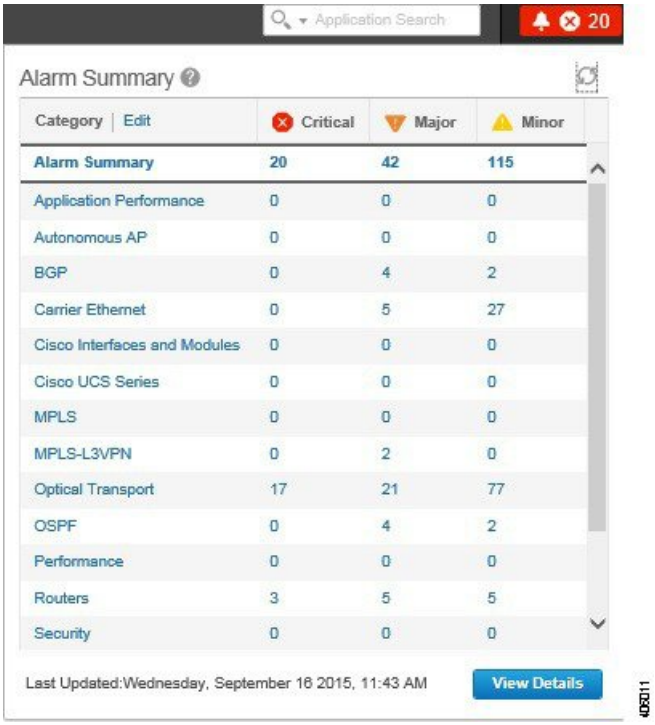
The notification is not enabled by default and needs to be enabled from the **My Preferences** page. For details on how to enable the critical alarm count notification, see Set Up Your Alarm and Event Display Preferences, on page 247.

Customize the Alarm Summary

You can specify what alarm categories are displayed:

- In the Cisco Evolved Programmable Network Manager title bar alarm count (bell). This gives you a quick visual count of alarms you are interested in.
- In the Alarm Summary pop-up window that is launched when you click the alarm count. The pop-up window gives you a quick look at alarm counts with their severity, as shown in the following figure.

Note Make sure that the pop-up blocker is disabled in the web browser where you are using EPNM.



To customize this information:

Step 1 Click **Edit** at the top left of the Alarm Summary pop-up window. This opens your My Preferences page. You can also open this page by clicking at the top right of web GUI window and choosing **My Preferences**.

Step 2 Click the **Alarms & Events** tab.

Step 3 To change the Alarm Summary refresh interval, select a number from the **Automatically Refresh Alarms & Events page** drop-down list.

Step 4 To specify what is included in the Alarm Summary, Go to the **Alarm Categories** area. Select **Alarm Summary** from the **Default category to display** drop-down list. Enable or disable the required Alarm Category by selecting or deselecting the corresponding checkbox.

Step 5 Click **Save** to confirm the changes made in the My Preferences window.

Interpret Event and Alarm Badges and Colors

When there is a problem in the network, Cisco Evolved Programmable Network Manager flags the problem by displaying an alarm or event icon with the element that is experiencing the problem. Alarm Severity Icons, on page 251 lists the icons and their colors.

Alarm Severity Icons

The table below lists the alarm colors and their respective severity levels for the icons displayed in various parts of the web GUI.

Severity Icon	Description	Color
	Critical alarm	Red
	Major alarm	Orange
	Minor alarm	Yellow
	Warning alarm	Light Blue
	Alarm cleared; normal, OK	Green
	Informational alarm	Medium Blue
	Indeterminate alarm	Dark Blue

Find and View Alarms

To view alarms, go to **Monitor** > **Monitoring Tools** > **Alarms and Events**. In the **Alarms** tab, alarms are listed in a table under the respective sub-tabs. Each of these tables displays a default set of columns. To enable a column that is not displayed by default, click ⚙ at the top-right corner of the table and select the column.

From the displayed alarms table, you can search for specific alarms, as described in the table below. To get more information about an alarm, see View an Alarm's Details, on page 258.

Note By default, acknowledged and cleared alarms are not included in any search criteria. This behavior is controlled by the system administrator. See Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms, on page 850

To find these alarms:	Choose Monitor > Monitoring Tools > Alarms and Events and:
Alarms generated by a specific device	For active alarms, click the ***i*** icon next to the device name to open the Device 360 view, then click the **Alarms** tab. For cleared alarms, refer to the Alarms and Events table. **Note** • For Cisco NCS 2000 series devices, transient conditions are processed as alarms and displayed in the Alarms table. Click ***i*** to navigate to the related port through the Interface 360 view. This feature is enabled only when you select the **Enable Transient Condition Alarms** check box in **Alarm Other Settings** page. Enabling the **Transient Condition Alarms** feature requires selecting the corresponding check box on the **Alarm Other Settings** page. If you disable this feature after an alarm has been triggered, the alarm will continue to be displayed on the **Alarms** tab. See Specify Alarm Clean Up, Display, and Email Options, on page 847) for more information. • For SVO devices, clicking the device name hyperlink cross launches the SVO UI. The SVO device hyperlink is enabled only if you have selected the **Enable Alarms Cross Launch to SVO** check box in the **Alarm Other Settings** page. See Specify Alarm Clean Up, Display, and Email Options, on page 847 for more information. For cleared alarms or correlated alarms, click the appropriate tab and enter the device name or component in the **Location** column. You can use wild cards. For certain devices, you can also use the Chassis View to check device alarms. See View Alarms in the Chassis View, on page 99.

To find these alarms:	Choose Monitor > Monitoring Tools > Alarms and Events and:
Alarms generated by a specific circuit/VC	1. Click the ***i*** icon next to the device name to open the Device 360 view, then click the **Circuit/VC** tab. 2. Click the ***i*** icon next to the Circuit/VC name to open the Circuit/VC 360 view, then click the **Alarms** tab. See Check Circuits/VCs for Faults, on page 659 for more circuit/VC alarm information.
All alarms in the network	Click the **Show Alarm History** link.
Alarms assigned to you	Click the **Show** drop-down filter list and choose **Assigned to me**. You can also use this filter in the Cleared/Correlated alarms tabs.
Unassigned alarms	Click the **Show** drop-down filter list and choose **Unassigned Alarms**. You can also use this filter in the Cleared/Correlated alarms tabs.
Cleared Alarms	Click the **Show** drop-down filter list and choose **Cleared Alarms** Alarms. You can also use this filter in the Cleared/Correlated alarms tabs.
Network Alarms	Under the **Alarms** tab, click **Network Alarms** tab to view all network impacting alarms. This tab is enabled only if you have selected the **Enable Network Alarms View** check box in **Alarm Other Settings** page. See Specify Alarm Clean Up, Display, and Email Options, on page 847 for more information.
Latest alarms according to the Cisco EPN Manager timestamp	For active alarms: • Alarms in the last 30 minutes—Click the Show drop-down filter and choose the last 5, 15, or 30 minutes **(CEPNM timestamp)**. • Alarms in the last 24 hours—Click the Show drop-down filter and choose the last 1, 8, or 24 hours **(CEPNM timestamp)**. • Alarms in the last 7 days—Click the Show drop-down filter and choose the last 7 days **(CEPNM timestamp)**. You can use these same filters for cleared and correlated alarms. The filters do not have the **(CEPNM timestamp)** suffix because filtering by device timestamps is not supported for cleared and correlated alarms. For more information on **(CEPNM timestamp)** and **(Device timestamp)**, see Device Timestamp and CEPNM Timestamp, on page 255.
Latest alarms according to the device timestamp	Follow the same instructions given in the previous row, but choose the filters with the suffix **(Device timestamp)** This filter is not supported when searching for cleared or correlated alarms.
All alarms generated by a device group, series, or type	Choose a group from the navigation pane on the left. You can also use this filter for cleared and correlated alarms.

You can also filter the data to find specific alarms using a *quick filter* or an *advanced filter* from the **Show** drop-down list.

Note Any optical alarm that is not supported for a device appears as **Optical Alarm** under the Alarm Conditions column.

Filter Data in the Alarms Table

You can filter the data to find specific alarms using a quick filter or an advanced filter from the **Show** drop-down list. The quick filter narrows the content that is displayed in a column according to the text you enter above the column. The advanced filter allows you to narrow down the data in a table by applying a filter using multiple operators such as Does not contain, Does not equal, Ends with, Is empty, and so on. You can also create a user-defined filter which, if saved, will be added to the **Show** drop-down menu.

Locally created root and admin users in EPNM have the option to create a public filter that can be shared with other users. They can also edit and delete public filters (created by either of them). The option to create a public filter is available only to root and admin users. Other users do not have this option and can only create private user-defined filters by default.

To create a user-defined filter:

Step 1 Click **Show** above the extended tables of alarms and choose **Advanced Filter**.

Step 2 In the Advanced Filter data popup window, enter the advanced filter criteria, and click **Save As**.

Step 3 In the **Save Filter** dialog box, enter a name for the filter and click **Save**.

a) **Root users only**: In the dialog box that appears, choose one of the following options :

- Choose **Public** if you wish to share the filter with other users. The newly created filter is added to the **Show** drop-down list under **Advanced Filters** and available to other users.
- Choose **Private** if you do not wish to share the filter with other users. The newly created filter is added to the **Show** drop-down list under **Advanced Filters** but not visible to other users.

(Root and admin users only): To edit or remove a user-defined filter, click **Show** > **Manage User Defined Filters**, select the user-defined filter and click **Edit** or**Remove**.

Create User-Defined Fields (UDF) for Custom Values in the Alarms table

You can create your own fields and define custom values in these fields to be displayed in the Alarms table. For example, to label certain alarms with a customer name. After you have created user-defined fields and assigned values, you can search for an alarm with these values in the Alarms table.

Note By design, Advanced Filters are not supported for user-defined fields (UDF).

To create a user-defined field for alarms:

Before you begin

To enable the user-defined fields, navigate to **Administration** > **Settings** > **System Settings** > **Alarms and Events** > **Miscellaneous** and select the check box for **Enable User Defined Field feature for alarms**.

To enable notifications for device UDFs, navigate to **Administration** > **Settings** > **System Settings** > **Alarms and Events** > **Miscellaneous** and select the check box for **Enable Device UDF to be sent in notifications**.

Step 1 Navigate to **Administration** > **Settings** > **System Settings** > **General** > **User Defined Fields**

Step 2 Click the **+** icon. Select **Alarms** from the drop-down list and enter a label and description.

To edit values in user-defined fields for alarms:

1. Navigate **Monitor** > **Monitoring Tools** > **Alarms and Events** > **Alarms**.
2. Click the settings icon at the top right of the table, choose **Columns**, then select your user-defined field from the list to display it as a column.
3. Select the check box of the corresponding alarm and click **Edit UDF**.
4. Enter the required value in user-defined field, and click **Save**.

Device Timestamp and CEPNM Timestamp

While **Device timestamp** is the information embedded inside the syslogs message, **CEPNM timestamp** is the time at which the message (from the device) is received at the Cisco EPN Manager end.

The following configuration is recommended on the device:

service timestamps log datetime show-timezone msec year

The default formats supported for device timestamps are:

- yyyy-MMM-dd HH:mm:ss.SSS z
- yyyy-MMM-dd HH:mm:ss z
- MMM-dd-HH:mm:ss z
- yyyy-MMM-dd HH:mm:ss.SSS
- yyyy-MMM-dd HH:mm:ss
- MMM-dd HH:mm:ss

Where **z** in the format implies a time zone.

Note Only three letter time zones are supported and time zones with hour/minute offsets are not supported.

Note The Cisco EPN Manager displays the time in the following standard format: **DD-MMM-YYYY hh:mm:ss AM/PM Z**, where Z is the time zone, irrespective of the device timestamp format. The same time format is followed throughout the Cisco EPN Manager GUI.

Standard time format example: 12-Dec-2022 12:10:11 AM IST

Track and Monitor Alarms

You can track and monitor alarms by setting the alarm auto-refresh interval to 10 seconds from the **Refresh** drop-down list. The list of alarms is refreshed and the latest 4000 alarms are displayed, along with the corresponding **Alarm ID**

View a Specific Alarm in the Topology Map

From the Alarms table, you can select a specific alarm and launch the topology map to see the alarm on the map.

Step 1 To display the Alarms table, choose **Monitor** > **Monitoring Tools** > **Alarms and Events**.

Step 2 In the Alarms tab, locate and select the required alarm.

Step 3 Choose **Troubleshoot** > **Network Topology**.

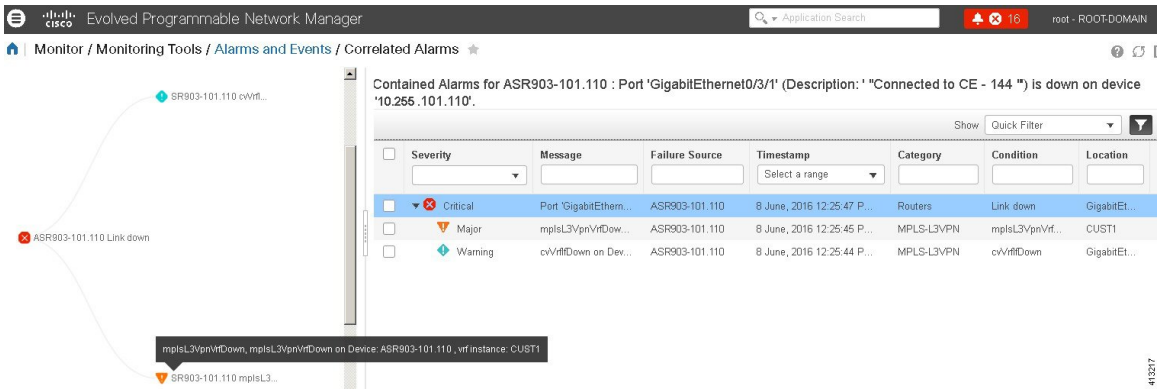
The view switches to the topology map and the device with the alarm is highlighted in the map.

View Root Cause and Correlated Alarms

The Cisco Evolved Programmable Network Manager correlation process determines the causality for alarms and alarm sequences. Alarms that support the correlation process are:

- A root cause alarm—An alarm that causes other alarms (the "correlating" alarm).
- A symptom alarm—An alarm that is the result of another alarm (the "correlated to" alarm).

Root cause and symptom alarms are displayed in a hierarchical manner to help you easily identify impacted network elements. The following figure is an example of an uncleared link down alarm that is the root cause for two other link down symptom alarms. To display an alarm tooltip in the hierarchy, hover your mouse over an alarm.



This view is especially helpful when alarm sequence has multiple hierarchies. All alarm sequences, regardless of the number of hierarchies, have only one root cause alarm.

To view *uncleared* correlated alarms,

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**.

Step 2 Click the **Correlated Alarms** tab.

Step 3 Click in the **Correlation Type** column to display more information about the alarm in a new view.

You can also view *uncleared* correlated alarms in the main Alarms and Events table. Click in the **Correlation Type** column to view more information about the alarm in a new view.

In this view, you can:

a. Perform actions such as Acknowledge and Clear the alarms. For more information, see Acknowledge and Clear Alarms, on page 260

b. Filter the list based on the severity, status and time stamp.

c. Choose the list of columns to be displayed by clicking at the top right corner of the table.

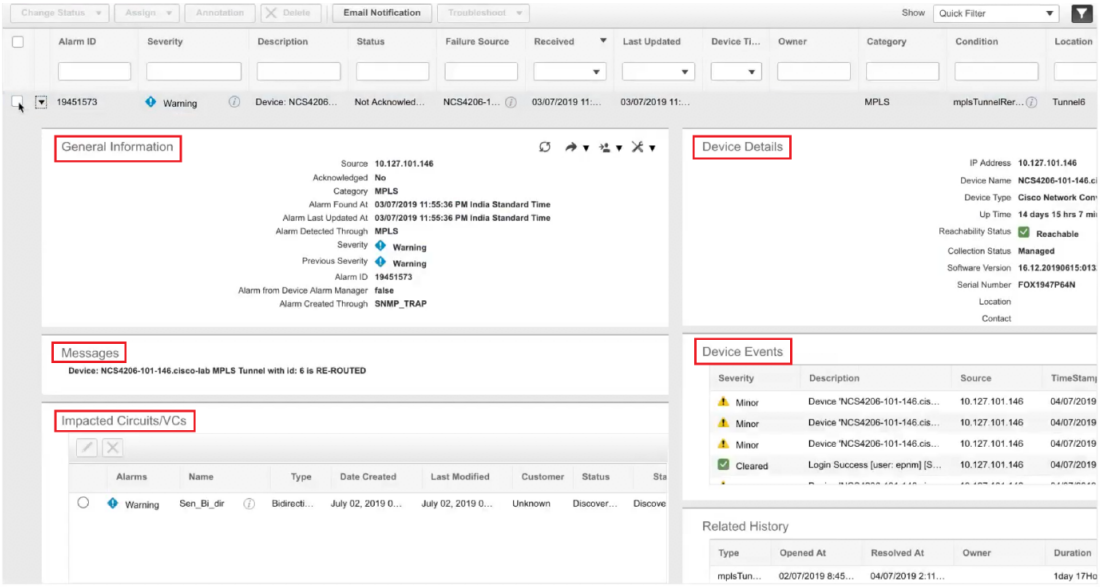
Cleared correlated alarms are displayed in the **Cleared Alarms** tab. Like *uncleared* alarms, the **Correlation Type** column will identify it as a cleared root cause alarm or symptom alarm.

Get Troubleshooting and Detailed Alarm Information

View an Alarm's Details

To get more details about an alarm, expand it. You can do this from the Alarms list (by choosing **Monitor** > **Monitoring Tools** > **Alarms and Events**, or by clicking **View Details** in the Alarm Summary pop-up). When you expand an alarm , the auto refresh of the table is paused. The circled areas are explained in the table that follows this figure.

Figure 10: View an Alarm's details



General Information—When alarm was found and last updated, current and last severity, alarm ID and how it was detected	**Device Details**—Managed device name, address, uptime, reachability status, collection status, and so forth
Messages—Trap, syslog, or TL1 message	**Device Events**—Recent device events from past hour (of any type, in chronological order)
Impacted Circuits/VCs—Carrier Ethernet or Optical circuits/VCs affected by alarm	

Find Troubleshooting Information for an Active Alarm

Use this procedure to get an explanation for why an active alarm occurred, and the recommended response to the alarm.

Note Not all alarms have this information. Users with sufficient privileges can add or change the information that is displayed in the popup window. See Customize the Troubleshooting Text for an Alarm, on page 853.

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**, then click the **Alarms** tab. (For interface alarms, you can also get this information from the Interface 360 view under the **Alarms** tab.)

Step 2 Locate the alarm, then click the "*i*" icon in the **Severity** column to open the popup window that provides the explanation and the recommended action that can be taken to troubleshoot the alarm.

If you take any actions, we recommend you document your actions. Choose the alarm, click **Annotation**.

Find Out Which Events Are Associated With An Alarm

To view the events that have been correlated to an alarm, from the Alarms table, click the “i” icon next to the Severity.

Find Out If An Alarm Impacts Other Services or Network Elements

The Alarms table contains a **Service Affecting** column which tells you if an alarm affects other parts of the network:

Note Service-affecting information is displayed for optical devices only.

- **SA** means it is a service-affecting alarm
- **NSA** means it is not a service-affecting alarm

To identify all alarms that can affect services, choose **Quick Filter** from the Show drop-down list and enter **SA** in the field above the Service Affecting column.

To find out which services are affected, expand the alarm and check the details in the Impacted Circuits/VCs area of the alarm details.

Alternatively, you can view the list of all the Service Affecting Alarms from the **Service Affecting** tab on the Alarms and Events page. This list has the service-affecting information for all the devices managed by Cisco EPN Manager. To navigate to the **Service Affecting** tab, choose **Monitor** > **Monitoring Tools** > **Alarms and Events**, then click **Service Affecting** tab.

Note There is no "**Showing Active Alarms**" option in this tab. By default, the entire list of alarms is displayed.

The Alarms table also contains a **Correlation Type** column which tells you if the alarm is causing other alarms (Root Cause Alarm), or if the alarm is a symptom of another alarm (Symptom Alarm). For more information, see View Root Cause and Correlated Alarms, on page 256.

Acknowledge and Clear Alarms

An alarm can have a status of Not Acknowledged, Acknowledged, or Cleared.

Not Acknowledged

Not Acknowledged means the problem is not being worked on. It could indicate that a new fault condition in the network, or that a cleared fault condition that has recurred. Not Acknowledged alarms are not removed from the Alarms and Events tables until they are either acknowledged or cleared.

Acknowledged

Acknowledged means a fault condition has either been recognized and is being worked on, or it can be ignored. Moving an alarm to the acknowledged status is a manual operation and changes the alarm Status to Acknowledged. An acknowledged event is still considered to be open (that is, not cleared), so if any related events recur, the events are added to the alarm.

By default, acknowledged alarms are not removed from the Alarms list. This behavior depends on the **Hide Acknowledge Alarms** setting that is controlled by the Administrator.

Acknowledged alarms can be moved back to the Not Acknowledged status (for example, if you acknowledged the wrong alarm).

Cleared

Cleared means the fault condition no longer exists. If an alarm is cleared but an associated event recurs, Cisco Evolved Programmable Network Manager opens a new alarm. An alarm can be cleared by a user or by the Cisco Evolved Programmable Network Manager system. Cleared alarms are removed from the Alarms list (but you can still view them under the Cleared Alarms tab).

By default, cleared alarms will not be shown in the Alarms and Events page. To view the cleared alarms in the Alarms History table in the Alarms and Events page:

Note When FRU alarms are generated, if inventory lacks location parameters then, generated alarms will not have location parameters. When the FRU alarms are cleared, the alarms may not have inventory location parameters.

- Choose **Administration** > **Settings** > **System settings**, then choose **Alarms and Events**.
- Under **Alarm Display Options**, uncheck the **Hide cleared Alarms** check box.

You can also clear an alarm by choosing **Clear all of this Condition**, which will clear all alarms that are having the same problem. You may also be prompted to change all alarms with that condition to Informational severity. This means that if an associated event recurs, a new alarm will *not* be opened. You should use that setting with care.

To change the status of an alarm:

Step 1 Choose **Monitor > Monitoring Tools > Alarms & Events**.

Step 2 Select an alarm, then choose **Change Status** and the appropriate status (Acknowledge, Unacknowledge, Clear, Clear all of this Condition).

Note **Clear all of this Condition** triggers a clearing event for *all alarms* with the same condition as the alarm you selected. When you choose this status, Cisco Evolved Programmable Network Manager displays a dialog asking if you want to change the severity for the selected alarm condition to Information. This prevents Cisco Evolved Programmable Network Manager from issuing alarms for the specified condition. To later reset the condition's severity, choose **Administration > Settings > System Settings > Alarm Severity and Auto Clear** and modify the severity. See Change Alarm Severity Levels, on page 853 for more information.

Step 3 Click **Yes** to confirm that you want to clear all alarms of the specified condition.

What are the Supported Alarm Clearing Mechanisms

At times you may face a situation where there are so many alarms that are available irrespective of their events being cleared. If you encounter any such problems, here are some of the solutions supported in Cisco Evolved Programmable Network Manager.

- Default clearing of alarms—The fault is resolved on the device and an event is triggered for the same. For example, a device-reachable event clears the device-unreachable event. This in-turn, clears the device-unreachable alarm.
- Auto-clearing of alarms—In some cases, a device may not generate a clearing alarm. In such cases, Cisco Evolved Programmable Network Manager waits for 24 hours (default interval) and then auto-clears the alarm. You need to have administrator privileges to change the auto-clear duration and to know how to set that interval, see Change Alarm Auto-Clear Intervals, on page 854.
- Clearing alarms based on inventory status of ports— When a device is rebooted, a card is reloaded or a RSP failover happens, the inventory collection is triggered for that device. During this inventory synchronization, Cisco Evolved Programmable Network Manager clears several types of alarms located on some specific ports based on the operational status of that particular port of the device. For example, when Cisco Evolved Programmable Network Manager receives a Link Down trap from a device, it generates a Link Down alarm on the specific port since it is operationally down. After a device reboot, if the operational status of the port changes to up, then the Link Down alarm is cleared automatically by Cisco Evolved Programmable Network Manager.
- Syncing device to clear alarms—Here, the devices are synced so that Cisco Evolved Programmable Network Manager gets the list of the outstanding active alarms and the events that does not exist are cleared. This is a different mechanism when compared to the event based alarm/event reporting (over traps/syslogs). Once the sync is over, the Alarms Table is refreshed to display only the outstanding active alarms.

Note This feature is supported only for certain devices or for certain device functionalities. For example, this feature is supported for optical devices/optical part of devices such as NCS 4K, NCS 1K.

Note This feature is also supported for certain packet devices such as NCS 42xx. See the Cisco Evolved Programmable Network Manager Supported Syslogs spreadsheet for the list of syslogs that are supported on the NCS 42xx devices. For the NCS 42xx devices, the alarm severity that is configured on the device will overwrite the alarm severity that is configured in the Cisco Evolved Programmable Network Manager (**Administration** > **Settings** > **System Settings** > **Alarms and Events** > **Alarm Severity and Auto Clear**). This feature is not supported for other packet devices such as ASR 9K and 9xx.

- Manual clearing of alarms—In situations where the clearing event is missing, you can manually clear an alarm by choosing the particular alarm, and changing its status to Clear. For more information, see the **Cleared** section under Acknowledge and Clear Alarms, on page 260.

Add Notes To an Alarm

The annotation feature allows you to add free-form text to the alarm, which is displayed in the Messages area of the alarm details. To add text to an alarm, choose the alarm in the Alarms and Events table, click **Annotation**, and enter your text. As with acknowledging, when you annotate an alarm, Cisco Evolved Programmable Network Manager adds your user name and the annotation time stamp to the Messages area of the alarm details.

Manage How Alarms are Triggered (Alarm Thresholds)

You can customize how often information is gathered (polling interval), the threshold value that indicates a problem, and whether Cisco Evolved Programmable Network Manager should generate an informational event or an alarm (of an severity) when a problem is detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies** > **My Policies** and select the policy you want to edit.

Step 2 Locate the parameter you want to change. You can search for the parameter by entering a string in the **Parameter** text box.

Step 3 To adjust the polling interval, select the new interval from the **Polling Frequency** drop-down list. To disable polling, choose **No Polling**. Note that some polling frequencies are applied to groups of parameters. Changing the group interval will change the polling for all settings in the group. If a policy does not have any thresholds or events associated with it, Cisco Evolved Programmable Network Manager prompts you to save the changes.

Step 4 To change a threshold value, expand the parameter and choose a value from the parameter's drop-down list.

Step 5 To specify what Cisco Evolved Programmable Network Manager should do when the threshold is surpassed, choose an alarm value from the parameter's drop-down list. You can configure Cisco Evolved Programmable Network Manager to generate an alarm of a specified severity, generate an informational event, or do nothing (if no reaction is configured).

Step 6 Click:

- **Save and Activate** to save and activate the policy immediately on the selected devices.
- **Save and Close** to save the policy and activate it at a later time.

View Events (Including Generic Events)

The Events tab displays supported and generic (unsupported) events. Supported events are events that Cisco Evolved Programmable Network Manager generates based on information about the network. It receives this network information either through syslogs and traps generated by devices, or through polling and inventory collection. This process is described in How are Alarms and Events Created and Updated?, on page 244. Generic events are events that Cisco Evolved Programmable Network Manager does not recognize. Rather than drop the events, Cisco Evolved Programmable Network Manager assigns the events a Minor severity (this severity is applied to all generic events; to change it, see Change Alarm Severity Levels, on page 853). If desired, you can customize the information displayed by generic events; see Customize Generic Events That Are Displayed in the Web GUI, on page 859. For information about supported events, see Which Events Are Supported?, on page 247.

Generic event processing is disabled by default. Users with Administrator privileges can disable or re-enable it.

The Events tab provides a variety of filters that you can use to find the information you are looking for. You can also create and save customized (preset) filters using the same procedure described in Find and View Alarms, on page 252. The following table lists some of the ways you can filter events.

To find these events:	**Select Monitor > Monitoring Tools > Alarms and Events, click the Events tab, and:**
All events in the network	Click the **Show Event History** hyperlink
Latest 4,000 Events	Click the **Show Active Events** hyperlink
All events generated by a device group, series, type, location group, or user-defined group	Choose a group from the left sidebar menu
Events in last *x* minutes, hours, or days	Click the **Show** drop-down filter list and choose the appropriate filter
Non-informational events generated in the last hour	From the **Show** drop-down filter list, choose **Non-info events in last hour**
Events using customized filters	Create and save an advanced filter (see Find and View Alarms, on page 252)

Configure an Event or a Syslog as an Alarm

You can configure an event to generate an alarm. The event can be a trap or a syslog.

To configure an event or a syslog as an alarm:

Step 1 Open the configuration file **PKT_INFRA-FM_EvenTypes.xml** under <XMP_HOME/conf/fault/event/eventTypes.

Step 2 Create a Bean ID with a unique alphanumeric string without any special characters or space, except "_" and "-".

Step 3 Set the name, message, and description as required.

Step 4 Set the following values as below:

- defaultCategory = Optical Transport
- defaultSeverity = Severity of the syslog you want to configure
- clearBy= Event

Step 5 Save the configuration file. The alarm for the event reflects under the **Alarms** tab under **Alarms and Events**, without the need to restart Cisco EPN Manager.

You can check the log file, **decap.core.java.log** to see syntax errors.

Note When you configure an event or a syslog as an alarm, you cannot clear the alarm using the GUI of Cisco EPN Manager. The alarm is automatically cleared when the corresponding event is cleared.

Export Alarms, Events or Syslogs to a CSV or PDF File

Use this procedure to save alarms, events or syslogs as a CSV or PDF file.

Step 1 Navigate to the data you want to export.

- Alarms—Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**, then click the **Alarms** or **Cleared Alarms** or **Correlated Alarms** tab. or **Service Affecting Alarms**.
- Events—Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**, then click the **Events** tab.
- Syslogs—Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**, then click the **Syslogs** tab.

Step 2 If you have a very large amount of data, apply a filter; otherwise the export process may take some time.

Step 3 Click at the top right of the table to open the **Export** dialog box.

Step 4 Choose CSV or PDF, click **OK**, and save the file.

To export the events for a particular alarm, in the **Alarms** tab, hover the mouse over the "i" icon next to the particular alarm. In the pop-up window that opens, click  at the top right corner to perform the export operation.

What is an Alarm Policy?

An Alarm Policy is a filtering method that allows you to control the alarms on network conditions, thereby reducing noise in the system. With Alarm policies, you can control the alarms generated in the network based on conditions you specify. To view the list of alarm policies, navigate to **Monitor > Monitoring Tools > Alarm Policies**. You can create, edit, delete, and rank alarm policies.

Alarm policy includes one or more conditions and an action. Cisco EPN Manager applies the action to any events or alarms that meet all the specified conditions.

Note Newly created alarm policies do not apply retrospectively on alarms generated prior to the policy creation.

You can create alarm policies to perform the following actions:

- Suppress alarms—Does not generate alarms for the selected events. But, events are created and saved normally.
- Suppress events and alarms—Does not create events and alarms.

Note For entsensor alarms, you must use the Alarm Policy feature to suppress the alarm by using the **Suppress Alarms** option. Do not use the **Suppress Alarms and Events** option.

Alarm Policy Ranks

Cisco EPN Manager determines the priority or execution order of an Alarm Policy based on its rank. When two or more policies apply to the same alarm or event, Cisco EPN Manager executes the Alarm Policy with a higher rank. By default, Cisco EPN Manager ranks alarm policies in the order in which they are created.

Points to remember when you rank the alarm policies are:

- Alarm policies are ranked in ascending order. So, a policy with a lower number has higher priority.

  For example, an alarm policy with rank 1 has higher priority than an alarm policy with rank 10.
- A policy with highest priority is applied first, followed by the next highest, and so on.
- Policies with a higher rank may affect the behavior of a policy with a lower rank or may even override the lower-ranking policy entirely.
- Cisco EPN Manager does not suppress alarms in the following instances if a higher-rank alarm suppression policy has already been applied to the event.

To change the rank of an Alarm Policy:

Step 1 Navigate to **Monitor** > **Monitoring Tools** > **Alarm Policies**.

Cisco EPN Manager lists the alarm policies in the order in which they are created.

Step 2 Select the Alarm Policy for which you want to change the ranking.

Step 3 Click the Move To icon and enter the ranking number in the Row field or click the Move up icon or Move down icon and change the ranking order.

View Alarm Policies

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarm Policies**.

All the alarm polices are listed in the this page.

Step 2 Click the Expand icon to view the policy details.

Create a New Alarm Policy

To create a new Alarm Policy:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarm Policies**.

Step 2 Click the Add icon and choose the policy type from the **Select A Policy Type** window.

The **Create a New Alarm Policy** wizard appears.

Step 3 In the **Policy Attributes** page, enter the Name, Description (optional), and choose the type of action you want to perform.

Step 4 Choose one of the following options under **Action Options** tab.

- Suppress Permanently.
- Display if the condition persists for this duration (minutes); and select the time duration using the time slider.

Note This tab is enabled only if you have chosen **Suppress Alarms** in step 3.

Step 5 Choose the Device groups.

If you do not select any device the policy applies to all devices.

Step 6 Choose the alarms or events that you want to suppress based on the action chosen in the **Policy Attributes** page.

Step 7 Click **Summary** to view the details of the policy. If you wish to change the settings, navigate to the respective page and make the desired changes.

Step 8 Click **Finish**.

Edit an Existing Alarm Policy

To edit an Alarm Policy:

Procedure

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarm Policies**.

Step 2 Choose the policy and then click the Edit icon.

Clicking this icon starts the **Edit Alarm Policy** wizard.

Step 3 In the **Policy Attributes** page, check and modify the Description if required.

Note You cannot edit the policy name and action chosen while creating the policy.

Step 4 The remaining steps in the **Edit Alarm Policy** wizard are same as the steps in **Create a New Alarm Policy** wizard. See Create a New Alarm Policy, on page 266.

Step 5 Click **Finish** to save the changes or click **Cancel** to discard.

Delete Alarm Policy

To delete the alarm policy:

Procedure

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarm Policies**.

Step 2 Choose the alarm policy which you wish to delete and click the Delete icon.

Step 3 Click **Yes** in the Delete Confirmation dialog box to delete, or **No** to cancel.

Alarms and Events Notification Policies

You can create policies for sending notifications on specific alarms of interest that are generated from particular device groups, to specific recipient groups.

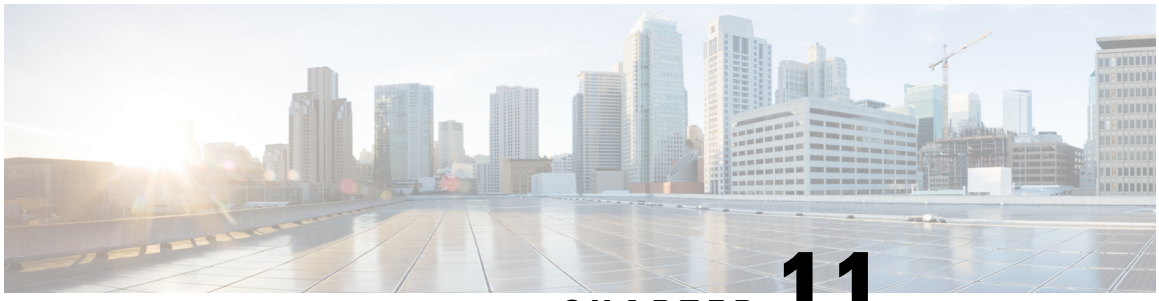
For more information see the section Event Receiving, Forwarding, and Notifications, on page 839 in the chapter Fault Management Administration Tasks.

Get Support from Cisco

If you receive an alarm in **Monitor > Monitoring Tools > Alarms and Events** for which you cannot find a resolution in the Cisco Support Community (click an alarm, then choose **Troubleshoot > Support Forum**.), you can use Cisco Evolved Programmable Network Manager to open a support request (click an alarm, then choose **Troubleshoot > Support Case**).

Respond to Problems Within Cisco Evolved Programmable Network Manager

Cisco Evolved Programmable Network Manager generates internal SNMP traps to monitor its own functions—such as server CPU and disk utilization, fan and power supply failures, and high availability (HA) state changes. For information on these types of events, see Troubleshoot Server Internal SNMP Traps, on page 777.



CHAPTER 11

Monitor Cisco ASR 9000 Network Virtualization (nV) Satellites and Cluster Services

Monitor Cisco ASR 9000 nV Satellites

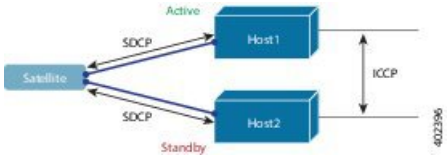
The Cisco ASR 9000 nV satellite feature set allows one or more smaller satellite switches to be interconnected with an Cisco ASR9000 device to form a single, combined access, aggregation and edge system.

Cisco Evolved Programmable Network Manager supports Cisco ASR 9000v, Cisco ASR 901, Cisco ASR 901S, Cisco ASR 903, and Cisco NCS 5001/2 devices as satellites. The Cisco ASR 9000v is a dedicated satellite switch that can only be used in nV satellite mode along with an Cisco ASR 9000 device. The Cisco ASR 901 and Cisco ASR 903 switches are “dual mode” switches. This means that they can operate both as standalone switches or as satellite switches within an nV system with an Cisco ASR 9000 device (in which case they are completely managed and controlled by the primary Cisco ASR 9000).

The satellite feature allows for both redundant and non redundant interconnections between the satellite switches and the primary Cisco ASR 9000s. The access side Ethernet ports of the satellite switches appear within the control and management planes of the host primary Cisco ASR 9000 just like locally connected Ethernet ports. All features that can be configured on the host Cisco ASR 9000 can also be configured and executed identically on satellite located ports. Effectively the satellite switches are *virtual line cards* of the host Cisco ASR 9000. Chassis management functions of the satellites such as software upgrades, inventory and environmental monitoring of hardware sensors (voltage, temperature etc) on the satellites are also seamlessly integrated into the same functions of the host Cisco ASR 9000, just like any other line card of the host Cisco ASR 9000 chassis.

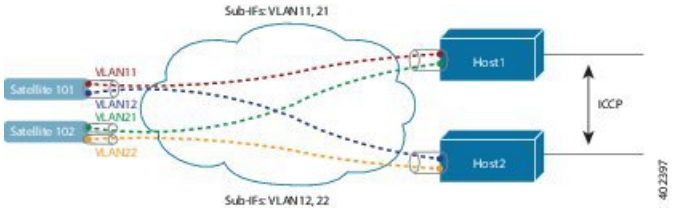
Cisco Evolved Programmable Network Manager supports the following types of nV Satellite configurations:

- Dual home hub and spoke (inventory support only)



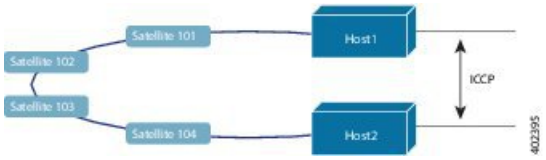
- The same satellite is dual homed to two separate Cisco ASR 9000 hosts – active and standby.
- Each host has an independent control channel with the satellite.
- The satellite is notified which host is active and which is standby.
- If the satellite loses its active host or link, failover occurs to its standby host.

- L2 fabric hub and spoke



- L2 Fabric supports satellite connectivity across Ethernet Layer 2 domains.
- Satellite Fabric Link Redundancy—single physical link with two VLANs/EVCs or two physical links with one VLAN/EVC each.
- Each host L2 subinterface is mapped to one satellite fabric port.

- Simple Ring



- Each satellite in the ring runs SDCP with two hosts independently.
- Each satellite maintains a logical hub-and-spoke topology over the physical ring topology.
- No local switching directly between satellites - all packets traverse the host.

Satellite Considerations in Cisco Evolved Programmable Network Manager

Satellites are not displayed in the Network Discovery page (**Inventory** > **Device Management** > **Network Devices**) because Cisco Evolved Programmable Network Manager does not support satellite device management operations from that page.

Satellites can only belong to Location groups because, as network nodes, they are normally managed according to location. In addition, if you add a host device to a group, its satellites are not automatically added to the group unless the group meets the following guidelines.

- If you use Add Devices Manually—From the create (or edit) group page, click Add, then choose All Locations from the Filter by drop-down list. The satellites will be listed if they match your criteria.
- If you use Add Devices Dynamically—Make sure you are creating a location group; and from the create (or edit) group page, choose All Locations from the Parent Group at the top of the page.

Minimum Device and OS Requirements for Cisco ASR 9000 nV Satellites

The following are the minimum device and device operating system requirements for the nV satellite feature set.

- Hardware — Cisco ASR 9000 Series Aggregation Services Routers with Cisco ASR 9000 Enhanced Ethernet line cards as the location of Inter Chassis Links and Cisco ASR9000v, Cisco ASR 901, Cisco ASR 903, Cisco NCS 5001, or Cisco NCS 5002 routers as satellite devices.

Note If the satellite is not an ASR 9000 device, its details will not be available in the host device's chassis view.

- Software — Cisco IOS XR 5.2.0.

Additional support may be available. For more information see the Cisco Evolved Programmable Network Manager.

Get Quick Information About a Specific Satellite: Satellite 360 View

The Satellite 360 view is a popup window that provides quick information about a satellite device, its inventory, and its status. This includes device alarms, modules, interfaces, and hosts.

To launch a Satellite 360 view:

- Click the "i" icon next to the device name in almost any device table
- From the network topology, click a device in an expanded group, then click **View**

The Satellite 360 view provides general satellite device information at the top of the view, and more detailed interface information in tabs in the lower part of the view.

Information Provided in Satellite 360 View	**Description**
General information	The satellite device type and name, status, last configuration change, and last inventory collection,
Modules	Modules that are configured on the satellite device, including their name, type, state, ports, and location.

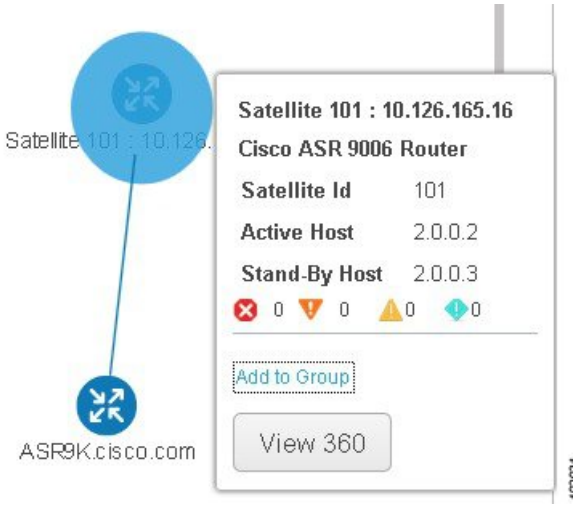
Interfaces	Name, operational and admin status for each associated satellite device . Also provides a launch point for the Interface 360 view. **Note** Subinterfaces for satellite devices are not listed under the Satellite 360 view.
Hosts	Name, IP address, and role (Active or Standby) of host devices that are connected to the satellite.

View Cisco ASR 9000 Host-Satellite Topologies in the Topology Map

You can visualize the Cisco ASR 9000 host-satellite topologies and see, at a glance, whether there are active alarms on the host or satellites. From the topology map you can drill down to get further information about the host and satellite devices.

You can easily identify a satellite in the map by its label which includes the satellite ID and the IP address of the Cisco ASR 9000 host.

Note To see the links between the devices in the satellite topology, you must enable the Inter-Chassis Control and ICCP links in the Link Types filter (top right corner above the map). ICCP protocol is used for host to host links.



To view Cisco ASR 9000 host-satellite topologies in the map:

Step 1 Choose **Maps >Topology Maps >Network Topology** in the left navigation pane.

Step 2 From the Groups pane on the left, select the group that contains the Cisco ASR 9000 host and satellites. The topology map displays all the devices in the selected group.

Step 3 Locate the host or one of the satellites in the map.

Step 4 To display the links between host and satellites:

- Click the filter icon in the topology toolbar and choose **Link Types**.

- Check the Control Plane, Inter_Chassis_Control, and ICCP check boxes, then click **OK**.

Step 5 Click a satellite to launch a popup showing the satellite ID as well as the ID of the active and standby hosts.

Step 6 Click View 360 in the popup to see more details about the satellite and its hosts in the Satellite 360 view, as described in Identify the Satellites Connected to a Cisco ASR 9000 Host, on page 273.

Identify the Satellites Connected to a Cisco ASR 9000 Host

The Device 360 view for a selected Cisco ASR 9000 host contains information about the device itself as well as about the satellites connected to the host.

To identify the satellites connected to a Cisco ASR 9000 host:

Step 1 Choose **Inventory >Device Management > Network Devices** in the left navigation pane.

Step 2 From the Device Group pane on the left, select the group that contains the Cisco ASR 9000 host.

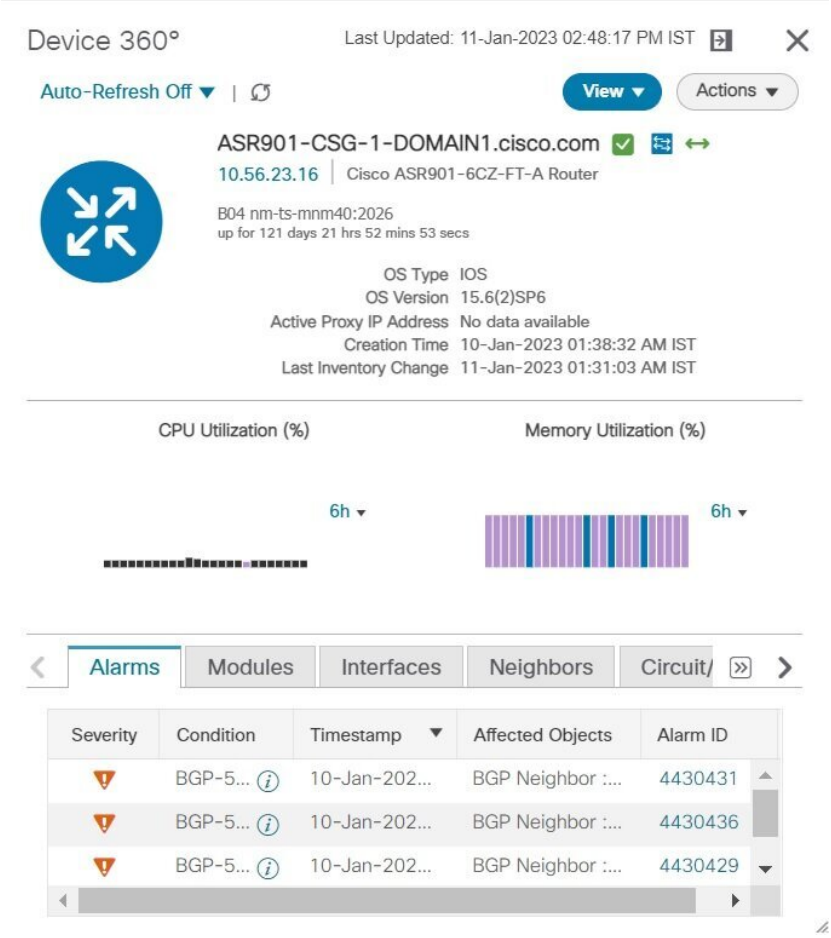
Step 3 Locate the host in the device list on the right.

Step 4 Click the "i" icon next to the device IP address/DNS to open the Device 360 view for the host.

Note You can also access the Device 360 view from the map by clicking on the device and then clicking **View 360** in the displayed popup.

The Satellites tab lists the satellites that are associated with the host and provides basic information about each satellite, such as type, description, IP address, and MAC address. It also indicates whether the satellite is currently connected to or disconnected from the host. The Satellites tab is only present in the Device 360 view for Cisco ASR 9000 host and satellite devices.

Step 5 Click the "i" icon next to the IP address in the Satellites tab to open the Device 360 view for the satellite. The Hosts tab lists the active and standby hosts associated with that satellite.



Identify the Hosts Connected to a Satellite

Usually the links in the map will clearly show the satellite topology including the host and the connected satellites. If for some reason the satellites are shown without links, it is easy to identify the hosts with which a satellite is associated.

To identify the hosts connected to a satellite:

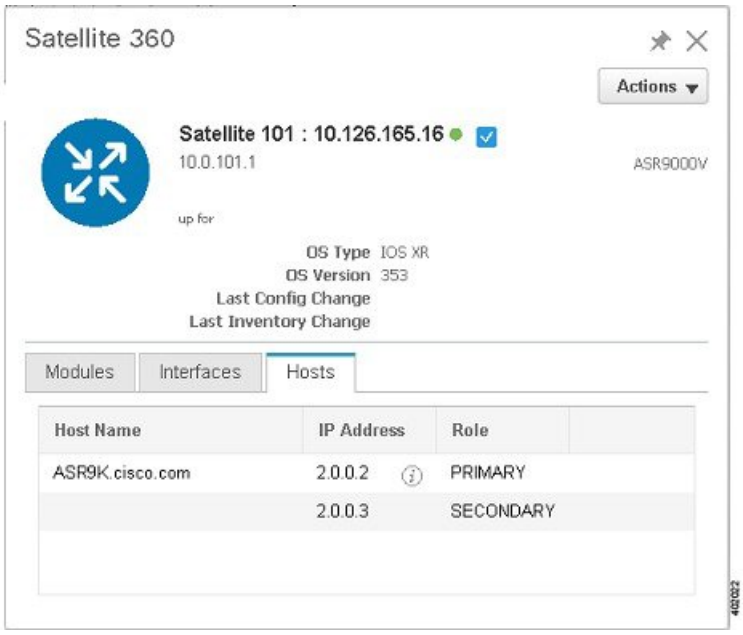
Step 1 Choose **Maps > Topology Maps Network Topology** in the left navigation pane.

Step 2 From the Device Groups pane on the left, select the group that contains the Cisco ASR 9000 host and satellites. The map displays all the devices in the selected group.

Step 3 Click a satellite device, identified by its label which begins with **Satellite ID**.

Step 4 In the displayed popup, click **View 360** to launch the Satellite 360 view.

The Hosts tab in the Satellite 360 view lists the host devices to which the satellite is connected and their role, either active or standby.



Monitor Cisco ASR 9000 nV Satellites for Faults

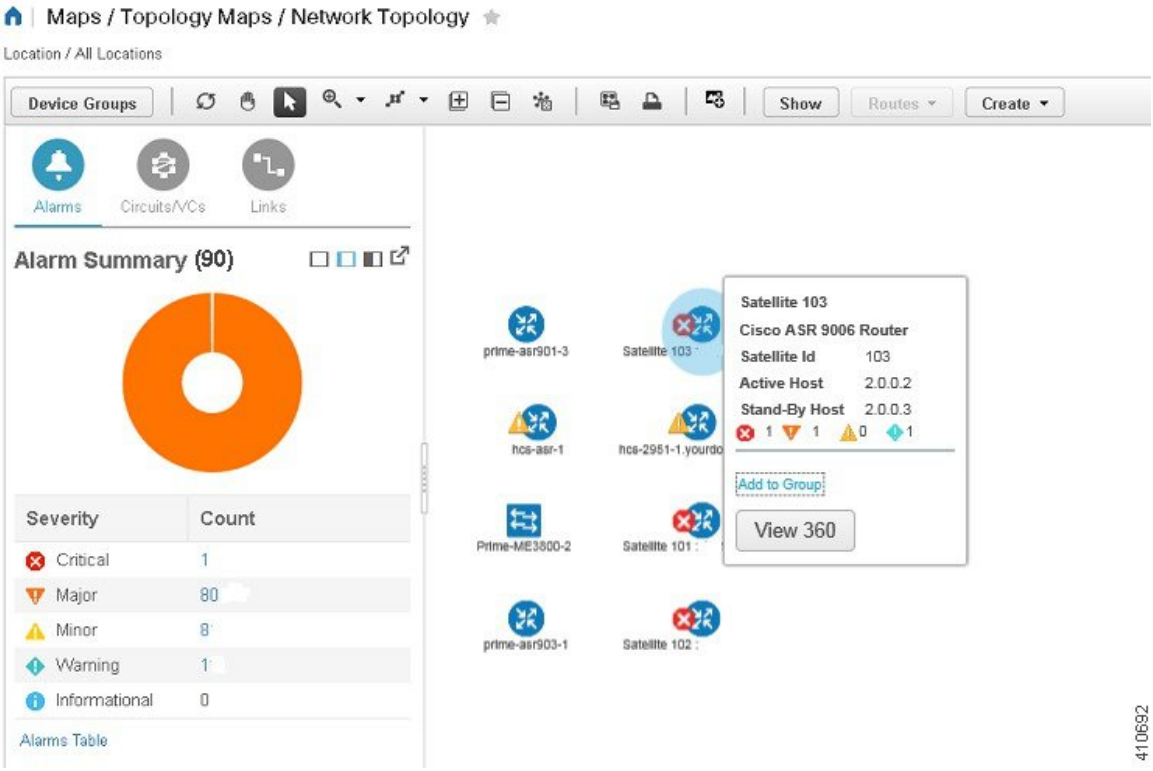
When a fault occurs on a satellite, Cisco Evolved Programmable Network Manager associates (localizes) the fault to either the host device or satellite device depending on the fault type.

- If a fault occurs on a physical entity, such as a port, fan, or module, Cisco Evolved Programmable Network Manager identifies the satellite device as the fault location.
- If the fault occurs on a logical entity such as a subinterface, Cisco Evolved Programmable Network Manager identifies the host device as the fault location because the subinterface is configured on the host.

If an alarm occurs on dual-homed satellite, the alarm is duplicated, with one alarm on the active host and another on the standby host.

View Satellite Faults in a Topology Map

In the topology map, you will see an alarm badge overlaid on the alarm source: the satellite device, the host device, or the link between the satellite and host device.

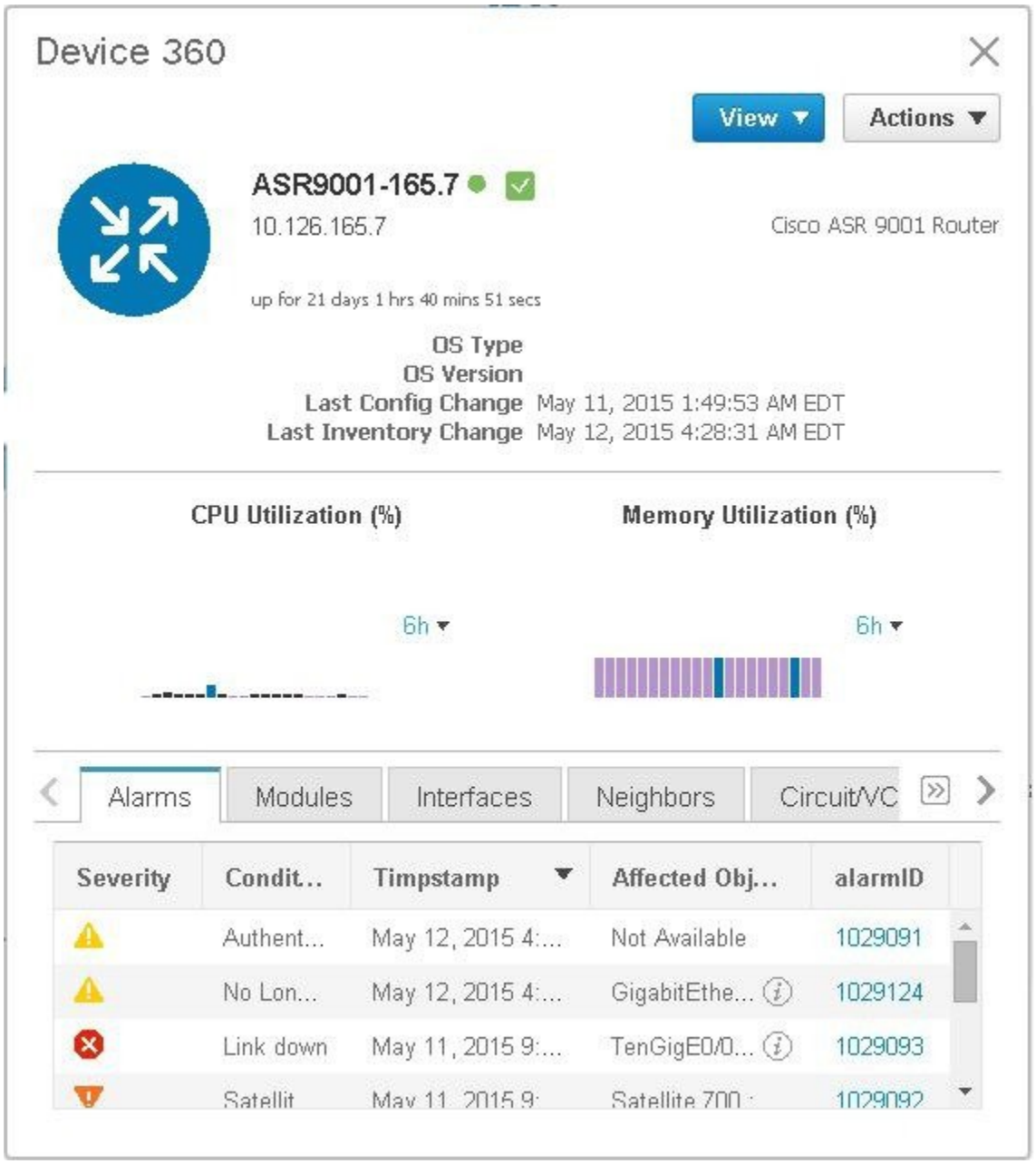


If there are several alarms on the same entity, the alarm badge severity represents that of the most severe alarm.

Right-click the alarmed entity to display a popup that shows the count of all active alarms related to the entity. Link-related alarms, such as Link Down, generate an alarm badge on the relevant link in the topology map.

View Satellite Faults Using a Device 360 View

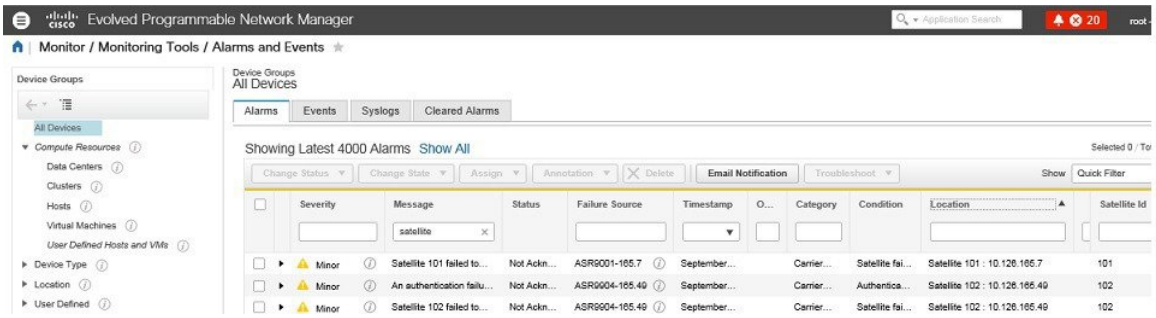
To find out which objects are affected by the device alarms, click View 360 from the popup menu and check the Affected Objects column. If you want to view details about a specific alarm, click the alarmID hyperlink.



View Satellite Faults in the Alarms and Events Table

To get satellite alarm information from the Alarm table, choose **Monitor** > **Monitoring Tools** > **Alarms and Events**, then click the **Alarms** tab.

Cisco Evolved Programmable Network Manager lists the host device as the Failure Source. The Satellite ID and Location fields identify the satellite source.



Monitor a Cisco ASR 9000 nV Edge Cluster

nV Edge is a feature where two or more Cisco ASR 9000 Series Router chassis are combined to form a single logical switching or routing entity. This allows you to operate two Cisco ASR 9000 Series Router platforms as a single virtual Cisco ASR 9000 Series system. Effectively, they can logically link two physical chassis with a shared control plane, as if the chassis were two route switch processors (RSPs) within a single chassis.

There are two types of links in the nV edge topology:

- Control links, used for control traffic.
- Inter-Rack links, used for data generation and forwarding of data between chassis.

Minimum Device and OS Requirements for nV Edge

The following are the minimum device and device operating system requirements for nV edge:

- 2 Cisco ASR 9000 devices running Cisco IOS XR 5.2.0
- 4 10G SFP (for IRL)
- 4 1G SFP (for cluster/control links)
- 2 RSP nodes per chassis, with the exception of the Cisco ASR 9001 which is a single RSP system that supports cluster configuration

Additional support may be available. See the Cisco Evolved Programmable Network Manager.

View a nV Edge Cluster in the Topology Map

The nV edge cluster is represented in the topology map as a single object consisting of two linked chassis, one primary and one backup.

To view the Cisco ASR 9000 nV Edge topology in the map:

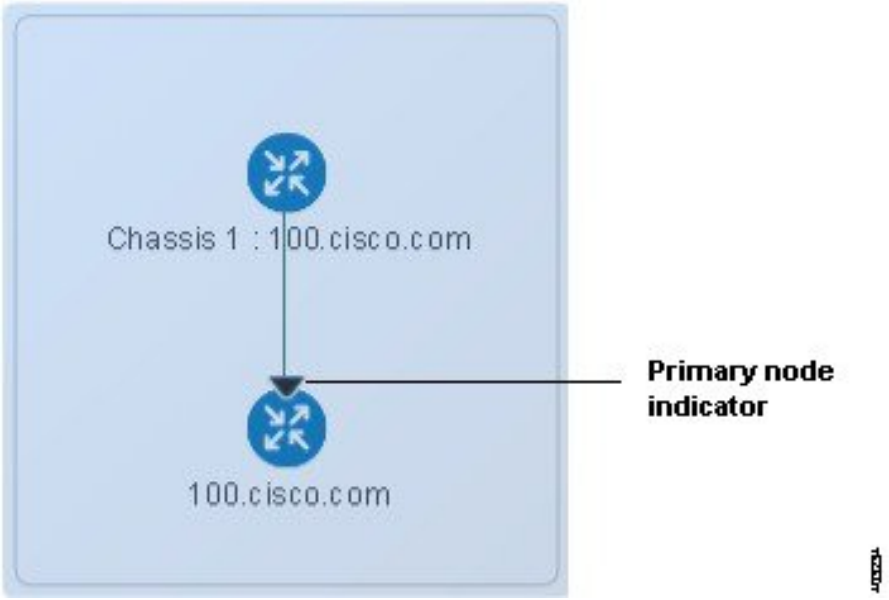
Step 1 Choose **Maps > Topology Maps> Network Topology** in the left navigation pane.

Step 2 From the Groups pane on the left, select the group that contains the Cisco ASR 9000 cluster. The topology map displays all the devices in the selected group.

Step 3 Click the primary or backup chassis. Note that both chassis are selected and a popup opens representing the two chassis together. You cannot access each chassis individually.

Step 4 To display links in the cluster topology:

- Click the filter icon in the topology toolbar, then choose **Link Types**.
- Check the Control Plane and Inter_Chassis_Control check boxes, then click **OK**.



Identify the Primary and Backup Devices in a Cluster

The topology map clearly shows which chassis is primary and which is the backup chassis. Further details about the chassis are provided in the Device 360 view.

To identify the primary and backup devices and get more information:

Step 1 Choose **Maps > Network Topology** in the left navigation pane.

Step 2 From the Device Groups pane on the left, select the group that contains the Cisco ASR 9000 cluster setup. The map displays all the devices in the selected group.

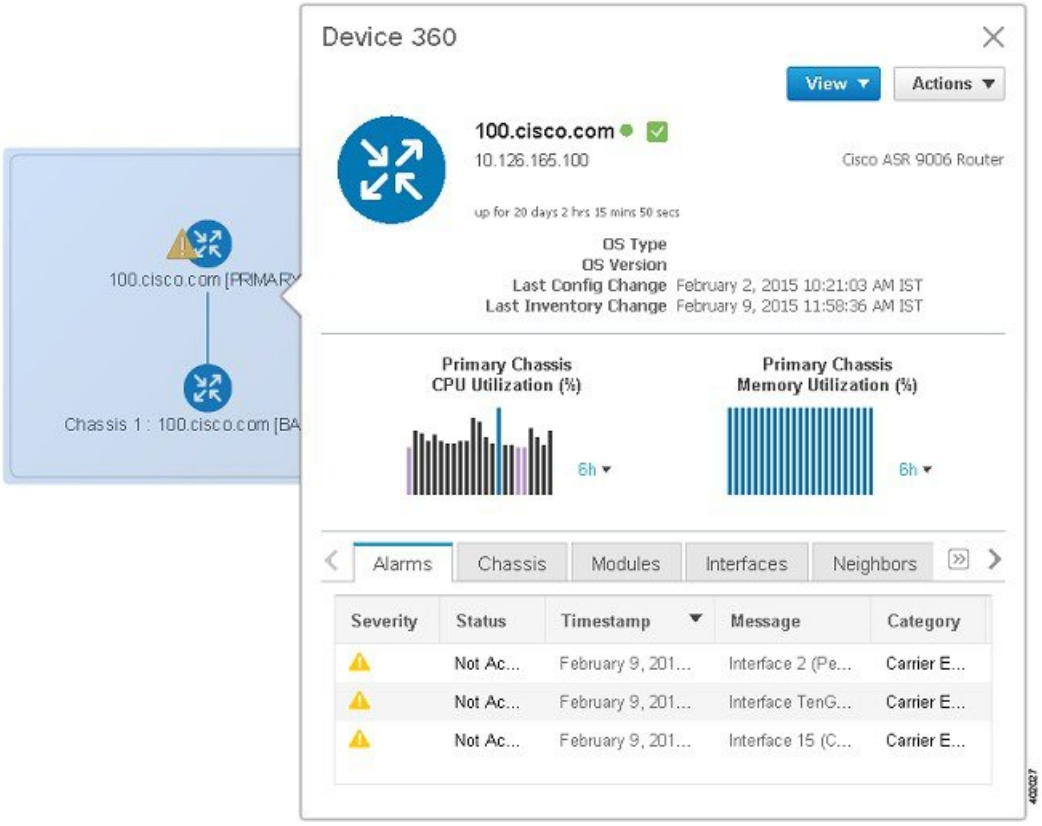
Step 3 Click the cluster representation.

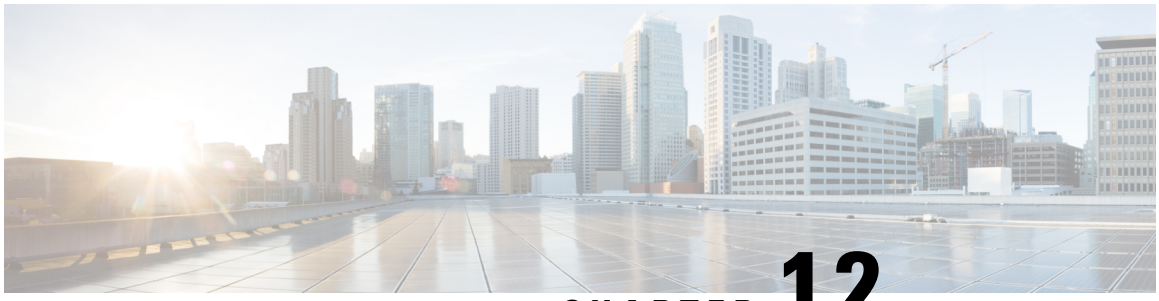
Step 4 In the displayed popup, click **View 360**.

Note that the Chassis tab in the Device 360 view lists and identifies the chassis in the cluster and provides information as to their status and their role (primary or backup).

Monitor and Troubleshoot a Cisco ASR 9000 nV Edge Cluster Service

Cisco Evolved Programmable Network Manager displays alarm indicators on the cluster and provides graphs showing CPU and memory utilization for the primary chassis in the Device 360 view.





CHAPTER 12

Manage Reports

Reports Overview

Cisco EPN Manager reports provide information about system, network health, and fault information. You can customize and schedule reports to run regularly. Reports can present data in a tabular, or graphical format (or a mixture of these formats). You can also save reports in XML, HTML, CSV, or PDF formats. The files can be saved on the Cisco EPN Manager server for later download, or sent to an e-mail address. To generate reports, see Create, Schedule, and Run a New Report, on page 302.

Cisco EPN Manager reports provide the following type of data:

- Current—provides a snapshot of data that is not time-dependent.
- Historical—periodically retrieves data from the device and stores it in the Cisco EPN Manager database.
- Trend—generates a report using aggregated data, which is collected and summarized as minimums, maximums, and averages.

With Cisco EPN Manager, you can filter these reports based on a specific criteria. For example, IPSLA Y.1731 reports can be filtered based on probes and PWE3 reports can be filtered based on Virtual Connection Identifier (VCID). You can also export reports, sort reports into logical groups, and archive reports for long-term storage.

Compress Report Files

You can choose to compress reports that exceed a particular file size limit. By default, any report that is larger than 5 MB is compressed in a zip format. To change the file size limit, update the variable `minSizeToCompressFile` in the `ReportResources.properties` file.

Step 1 Log in to Cisco EPN Manager as a CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Step 2 Open the `ReportResources.properties` file.

File path - `/opt/CSCOlumos/conf/rfm/classes/com/cisco/server/resources/ReportResources.properties`

Step 3 Update the `minSizeToCompressFile` with the required value (in bytes).

For example, if you wish to compress files larger than 7MB, update the variable as:

```
minSizeToCompressFile=7340032
```

Step 4 Save the file.

You need to restart Cisco EPN Manager for this change to take effect.

Available Reports

The **Reports Launch Pad** provides access to several Cisco EPN Manager reports. You can access them by navigating to **Reports** > **Reports** > **Reports Launch Pad**, and click the **Templates** tab. The reports available are:

- Carrier Ethernet Performance Reports, on page 283
- Device Reports, on page 291
- Network Summary Reports, on page 295
- Optical Performance Reports, on page 296
- Performance Reports, on page 301
- System Monitoring Reports, on page 302

You can choose to switch to **All Template** view which conatins all the reports, **Recently Used** view which contains a maximum of 20 recent reports which has been run, saved or scheduled or **Starred** view which contains all the reports which has been marked with a star to set a favorite. You can also refine and filter your reports by category or type from the left hand panel or search for a report using the search text box.

All the available reports are displayed in the center pane. You can add a favourite report by clicking on the star icon.

If you click on a report wideget, you will be redirected to the **Generated Reports** page where you can view the saved and scheduled reports for that paticular selection.

Carrier Ethernet Performance Reports

This section lists the Carrier Ethernet (CE) Performance reports supported by Cisco EPN Manager. It also includes the monitoring policies that must be enabled so that the proper report data is collected. For more information about monitoring policies, see How Device Health and Performance Is Monitored: Monitoring Policies, on page 223.

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
IPSLA Graphs	Graphical representation of average delay backward, average delay forward, average delay two-way, jitter forward, jitter backward, average backward packet loss ratio, average forward packet loss ratio, and availability.	*IPSLA* For details about the IPSLA monitoring policy, see IP SLA Monitoring Policy, on page 953.	Response Time Avg, Response Time Max,Response Time Min, Jitter Neg DS Avg, Jitter Neg SD Avg, Jitter Pos DS Avg, Jitter Pos SD Avg, Packet Loss Overall Util Avg, Packet Loss DS Util Avg, Packet Loss SD Util Avg, Latency One Way SD Avg, Latency One Way SD Max, Latency One Way SD Min, Latency One Way DS Avg, Latency One Way DS Max, Latency One Way DS Min
IPSLA Statistics	Tabular representation of probe index, IPSLA probe type, TOS, target IP, VRF name, average delay two-way, average delay forward, average delay backward, packet loss ratio forward, packet loss ratio backward, average jitter forward, average jitter backward, average backward packet loss ratio, average forward packet loss ratio, and availability.	*IPSLA* For details about the IPSLA monitoring policy, see IP SLA Monitoring Policy, on page 953.	Jitter Neg DS Avg, Jitter Neg SD Avg, Jitter Pos DS Avg, Jitter Pos SD Avg, Packet Loss Overall Util Avg, Packet Loss DS Util Avg, Packet Loss SD Util Avg, Latency One Way SD Avg, Latency One Way SD Max, Latency One Way SD Min, Latency One Way DS Avg, Latency One Way DS Max, Latency One Way DS Min

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
IPSLA Top N	Tabular representation of probe index, IPSLA probe type, TOS, target IP, VRF name, average delay two-way, maximum delay two-way, minimum delay two-way, average delay forward, maximum delay forward, minimum delay forward, average delay backward, maximum delay backward, minimum delay backward, average forward packet loss ratio, average backward packet loss ratio, jitter forward, jitter backward and availability.	*IPSLA* For details about the IPSLA monitoring policy, see IP SLA Monitoring Policy, on page 953.	Response Time Avg, Response Time Max,Response Time Min, Jitter Neg DS Avg, Jitter Neg SD Avg, Jitter Pos DS Avg, Jitter Pos SD Avg, Packet Loss Overall Util Avg, Packet Loss DS Util Avg, Packet Loss SD Util Avg, Latency One Way SD Avg, Latency One Way SD Max, Latency One Way SD Min, Latency One Way DS Avg, Latency One Way DS Max, Latency One Way DS Min
IPSLA Y.1731 Graphs	Graphical representation of average delay backward, average delay forward, jitter two-way, jitter forward, jitter backward, average backward frame-loss ratio, average forward frame-loss ratio, and availability of the Y.1731 probe. **Note** A value of –1 in *Probe Index*column indicates that the device does not have a Probe Index configured.	*IPSLA Y.1731* For details about the IPSLA Y.1731 monitoring policy, see IP SLA Y.1731 Monitoring Policy, on page 951.	Average Delay Two Way, Average Delay Forward, Average Delay Backward, Average Positive Jitter Forward, Average Negative Jitter Forward, Average Positive Jitter Backward, Average Negative Jitter Backward, Average Forward Frame Loss Ratio, Average Backward Frame Loss Ratio

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
IPSLA Y.1731 Statistics	Tabular representation of operation type, CFM domain, source, destination, frame type, average delay two-way, average delay forward, average delay backward, average jitter, forward frame loss ratio, backward frame loss ratio, average forward jitter, average backward jitter, and availability of the Y.1731 probe.	*IPSLA Y.1731* For details about the IPSLA Y.1731 monitoring policy, see IP SLA Y.1731 Monitoring Policy, on page 951.	Average Delay Two Way, Average Delay Forward, Average Delay Backward, Average Forward Frame Loss Ratio, Average Backward Frame Loss Ratio, Average Jitter
IPSLA Y.1731 Top N	Tabular representation of operation type, CFM domain, source, destination, frame type, average delay two-way, maximum delay two-way, minimum delay two-way, average delay forward, maximum delay forward, minimum delay forward, average delay backward, maximum delay backward, minimum delay backward, average forward frame loss ratio, maximum forward frame loss ratio, minimum forward frame loss ratio, average backward frame loss ratio, maximum backward frame loss ratio, minimum backward frame loss ratio, jitter forward, jitter backward, and availability of the devices that are configured using the Y.1731 technology.	*IPSLA Y.1731* For details about the IPSLA Y.1731 monitoring policy, see IP SLA Y.1731 Monitoring Policy, on page 951.	Average Delay Two Way, Average Delay Forward, Average Delay Backward, Average Positive Jitter Forward, Average Negative Jitter Forward, Average Positive Jitter Backward, Average Negative Jitter Backward, Average Forward Frame Loss Ratio, Average Backward Frame Loss Ratio

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Interface Availability	Displays the interface details for the devices in the network.	*Interface Health* For details about the Interface Health monitoring policy, see Interface Health Monitoring Policy, on page 950.	Statistics
Interface Graphs	Graphical representation of the interface traffic statistics over time: in traffic, out traffic, in utilization and out utilization.	*Interface Health* For details about the Interface Health monitoring policy, see Interface Health Monitoring Policy, on page 950.	Statistics
Interface Top N	Tabular representation of Top N reports of interface traffic statistics: maximum in traffic, average in traffic, maximum out traffic, average out traffic, maximum in utilization, maximum out utilization and current in utilization, current out utilization, in errors, out errors, in discards, out discards and interface availability.	*Interface Health* For details about the Interface Health monitoring policy, see Interface Health Monitoring Policy, on page 950.	Statistics
Interface Traffic	Tabular representation of interface traffic statistics: in traffic rate, out traffic rate, in utilization, out utilization, in errors, out errors, in discards, out discards, in packets rate, out packets rate (including L3 packets), CRC errors and percentage.	*Interface Health* For details about the Interface Health monitoring policy, see Interface Health Monitoring Policy, on page 950.	Statistics and CRC

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Link Optical SFP Power Level	Tabular representation of the A end device, A end interface, Z end device, Z end interface, and their Tx and Rx power levels. **Note** The prerequisite for this report is to have CDP/LLDP enabled links in the network.	*Optical SFP* For more details about the Optical SFP monitoring policy, see Optical SFP Monitoring Policy, on page 956.	Optical Tx Power, Optical Rx Power
Link Utilization	Tabular representation of A device name, A interface name, A member of, A end in utilization, A end out utilization, A end capacity, Z device name, Z interface name, Z member of, Z end in utilization, Z end out utilization, Z end capacity, event time, and the interface utilization of the interfaces participating in the link, including the link aggregate group they belong to. **Note** The prerequisite for this report is to have CDP/LLDP enabled links in the network.	*Interface Health* For details about the Interface Health monitoring policy, see Interface Health Monitoring Policy, on page 950.	Statistics

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
MPLS Link Statistics	Representation of link delay and jitter in MPLS segment routing.	*MPLS Link Performance* For more details about the MPLS monitoring policy, see MPLS Link Performance Monitoring Policy, on page 954.	Average Delay, Min Delay, Max Delay, RX Packets, TX Packets
Optical SFP Interface	Tabular representation of transmit/receive power levels of the devices for interfaces. Includes device name, interface name, RxPower, TxPower, EVENTTIME.	*Optical SFP* For more details about the Optical SFP monitoring policy, see Optical SFP Monitoring Policy, on page 956.	Optical Tx Power, Optical Rx Power
Optical SFP Threshold	Displays the sensitivity values that are statically configured and threshold values from OPTICALSFP_SETTINGS table.	*Optical SFP* For more details about the Optical SFP monitoring policy, see Optical SFP Monitoring Policy, on page 956.	All
PWE3 Statistics	Tabular representation of PWE3 traffic and availability statistics including device name, IP address, VC ID, peer address, VC type, current in bit rate, current out bit rate, current in byte rate, current out byte rate, current in packet rate, current out packet rate, global availability, in availability and out availability.	*Pseudowire Emulation Edge to Edge* For details about the Pseudowire Emulation Edge to Edge monitoring policy, see Pseudowire Emulation Edge to Edge Monitoring Policy, on page 952.	PW VC Perf Total In HC Packets Rate,PW VC Perf Total In HC Bytes Rate, PW VC Perf Total Out HC Packets Rate, PW VC Perf Total Out HC Bytes Rate, PW VC Oper Status Up, PW VC Inbound Oper Status Up, PW VC Outbound Oper Status Up, PW VC Oper Status Down, PW VC Perf Total In HC Packets, PW VC Perf Total In HC Bytes, PW VC Perf Total Out HC Packets, PW VC Perf Total Out HC Bytes, PW VC Inbound Oper Status Down, PW VC Outbound Oper Status Down

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
PWE3 Top N	Tabular representation of Top N reports of PWE3 statistics including device name, IP address, VC ID, peer address, VC type, average in byte rate, average out byte rate, maximum in byte rate, maximum out byte rate, average in bit rate, average out bit rate, maximum in bit rate, maximum out bit rate, average in packet rate, average out packet rate, maximum in packet rate, maximum out packet rate, global inbound availability and global outbound availability.	*Pseudowire Emulation Edge to Edge* For details about the Pseudowire Emulation Edge to Edge monitoring policy, see Pseudowire Emulation Edge to Edge Monitoring Policy, on page 952.	PW VC Perf Total In HC Packets Rate,PW VC Perf Total In HC Bytes Rate, PW VC Perf Total Out HC Packets Rate, PW VC Perf Total Out HC Bytes Rate, PW VC Oper Status Up, PW VC Inbound Oper Status Up, PW VC Outbound Oper Status Up, PW VC Oper Status Down, PW VC Perf Total In HC Packets, PW VC Perf Total In HC Bytes, PW VC Perf Total Out HC Packets, PW VC Perf Total Out HC Bytes, PW VC Inbound Oper Status Down, PW VC Outbound Oper Status Down
PWE3 Traffic Graphs	Graphical representation of PWE3 traffic including average in bit rate, average out bit rate, average in byte rate, average out byte rate, average in packet rate, average out packet rate, global availability, in availability and out availability.	*Pseudowire Emulation Edge to Edge* For details about the Pseudowire Emulation Edge to Edge monitoring policy, see Pseudowire Emulation Edge to Edge Monitoring Policy, on page 952.	PW VC Perf Total In HC Packets Rate,PW VC Perf Total In HC Bytes Rate, PW VC Perf Total Out HC Packets Rate, PW VC Perf Total Out HC Bytes Rate, PW VC Oper Status Up, PW VC Inbound Oper Status Up, PW VC Outbound Oper Status Up, PW VC Oper Status Down, PW VC Perf Total In HC Packets, PW VC Perf Total In HC Bytes, PW VC Perf Total Out HC Packets, PW VC Perf Total Out HC Bytes, PW VC Inbound Oper Status Down, PW VC Outbound Oper Status Down

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
QoS Policing	Tabular representation of the details about the policy map: ClassMap. The details include, direction of the policy map, average exceed byte rate, maximum exceed byte rate, maximum exceed date, average violate byte rate, maximum violate byte rate, maximum violate date, average conformed byte rate, maximum conformed byte rate, maximum conformed date, CIR current rate and PIR current rate. Also, graphical representation of exceed, violate and conformed byte rates.	*Quality of Service* For details about the Quality of Service monitoring policy, see Quality of Service Monitoring Policy, on page 952.	Conformed Bytes Rate, Exceeded Bytes Rate, Violated Bytes Rate, Exceeded Packets, Violated Bytes, CIR, Conformed Bytes, Exceeded Bytes, PIR

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
QoS Policy	Graphical and tabular representation of the details about the policy map: ClassMap. The details include, direction of the policy map, average pre-policy byte rates, maximum pre-policy byte rates, average post-policy byte rates, maximum post-policy byte rates, maximum pre-policy dates, maximum post-policy dates, average drop in percentage, maximum drop in percentage, maximum drop date, average pre-policy of CIR, average interface speed in percentage, maximum pre-policy of CIR, maximum interface speed in percentage, average pre-policy of CIR, maximum pre-policy of CIR and interface speed date. Also, graphical representation of pre-policy, post-policy, drop bit rate, and drop percentage.	*Quality of Service* For details about the Quality of Service monitoring policy, see Quality of Service Monitoring Policy, on page 952.	Drop Bytes Rate, Drop Percent, Post-Policy Bytes Rate, Pre-Policy Bytes Rate, Pre-Policy Percent of CIR, Post-Policy Percent of CIR, CIR, Post-Policy Rate (Bytes/Sec),Pre-Policy Bytes

Device Reports

This section lists the device reports supported by Cisco EPN Manager. It also lists the monitoring policies and parameters that must be enabled for each of the report type. These reports are applicable for both Optical and Carrier Ethernet technologies.

Note Report types marked with an asterisk (*) are applicable for SVO and Cisco NCS 2000 series devices.

For more information about monitoring policies, see Monitor Device and Network Health and Performance, on page 223.

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Alarm	List of alarms for devices in the network. Includes severity, message, status, failure source, time stamp, creation time, device timestamp, owner, category, condition, location, service affecting, satellite ID.	NA	NA
CPU Utilization	Table listing all devices with their average CPU usage for a specified time period.	*Device Health* For details about the Device Health monitoring policy, see Device Health Monitoring Policy, on page 949.	CPU Utilization
Detailed Hardware *	Hardware information for the entire inventory or device types (for example, Switches and Hubs, Routers, and Optical Transport).	NA	NA
Detailed Software *	Software information for the entire inventory or device types (for example, Switches and Hubs, Routers, and Optical Transport).	NA	NA
Device Availability	Table listing all the available devices in the network and their reachability percentage.	NA	NA
Device Credential Verification	The credential status of the devices in your network. Includes the login, reachability, and protocol statuses of each device. Also, includes the last modified date and time for the device.	NA	NA
Device Health	CPU utilization, memory utilization, and availability information of the network devices for a specified time period. Includes minimum, maximum, and average for all CPU modules and memory pools on a device.	*Device Health* For details about the Device Health monitoring policy, see Device Health Monitoring Policy, on page 949.	CPU Utilization
Device Serial Number	Lists the serial number of devices present on your network.	NA	NA
Event	List of events for devices in your network. Includes description, failure source, time stamp, device timestamp, severity, category, condition.	NA	NA

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
GNSS Module Inventory	GNSS inventory data like Satellite ID, Signal-to-Noise Ratio, Module status, Satellite Status, and Antenna Alarm status.	*GNSS Monitoring Policy* For details about the GNSS monitoring policy, see GNSS Monitoring Policy, on page 968.	NA
Identity Capability	Identity capability summary information for the switches in the network.	NA	NA
Interface Detail (Two report options are available: *Physical Interface* and *IP Interface*)	*Physical Interface Report*: Physical interface details of the devices in your network. Includes device name, port name, port description, MAC address, admin status, and operational status. *IP Interface Report*: Logical port data of the devices in your network. Includes device name, port name, port IP address, port description, admin status, and operational status.	NA	NA
Inventory *	Basic Inventory data for the devices in your network for each of the following categories: Combined Inventory, APs, Autonomous APs, Controllers, MSEs, Switches, Routers, Dead Radios, Cisco Interfaces and Modules, Storage Networking, Security and VPN, Optical Networking.	NA	NA
Link	Performance information related to OTU, OTS, ODU and OMS enabled links in a network.	*Device Health* For details about the Device Health monitoring policy, see Device Health Monitoring Policy, on page 949.	NA
Memory Utilization	Memory utilization information for a specified time period. Includes information for all memory pools/modules.	*Device Health* For details about the Device Health monitoring policy, see Device Health Monitoring Policy, on page 949.	Memory Pool Utilization

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Network Inventory Detail	Network inventory information in the network includes device name, device IP, equipment type, operation status, actual equipment type, physical location, CLEI code, hardware part number, manufactured date, serial number, product ID, version ID, and also UDFs (if selected from the column list under Settings tab).	*Device Health* For details about the Device Health monitoring policy, see Device Health Monitoring Policy, on page 949.	NA
Port Capacity	Percentage for interface utilization for devices in a network for the following report Types: All, Connected, Free, or Free Down.	NA	NA
PTP State	PTP Clock Class, PTP Servo, Port Index, and PTP Boundary Clock data.	PTP/SyncE Monitoring Policy For details about the PTP/SyncE Monitoring Policy, see PTP/SyncE Monitoring Policy, on page 952.	NA
PWID Inventory	List the Pseudowire Identifier (PWID) between all the local device and peer devices. Lists all PWID for all services per domain and per router.	*Device Health* For details about the Device Health monitoring policy, see Device Health Monitoring Policy, on page 949.	NA
SFP Port and Module Details	Lists the small form-factor pluggable and module details on your network.	NA	NA
Third Party Devices Detail	Lists the details of the third-party devices on your network.	NA	NA
Vlan	Vlan information for switches in a network.	NA	NA
VLAN Detailed	Detailed VLAN information for the switches in the network. Includes VLAN ID, VLAN name, VTP domain name, admin status, device IP address, device name, Interface IP address, operational VLAN mode, and operational status.	NA	NA

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Wired Detailed Device Inventory *	Detailed inventory data for the wired devices in your network. Includes system information, chassis information, module information, module port interfaces, VLAN interfaces, software image information, memory pool information, flash devices, flash partition, flash file. **Note** Up to 5 devices can be selected if you want to run the report immediately without saving it. To include more than 5 devices, save or schedule the report.	NA	NA
Wired Device Availability	List of wired devices with the highest and lowest availability in your network. Includes device name, average availability (%). **Note** This report is not applicable for SVO devices.	NA	NA
Wired Module Detail *	Table listing detailed module information for wired devices in the network including device name, device IP, equipment name, number of ports, operational status, vendor equipment type, manufacturer, serial number, and UDI.	NA	NA
Wired Port Attribute	Port attribute information such as admin status, operational status, MAC address, and so on. Includes VLAN ID, access mode VLAN, device IP address, Interface IP address, description, MAC address, Admin status, operational status, type, MTU, speed, duplex, IsTrunk, and trunk encapsulation *Wired Port Pluggable Attribute* is a sub-report type available under the Wired Port Attribute. It includes port pluggable attribute information, such as pluggable model information, pluggable description, pluggable type, port name, device IP address, interface IP address, MAC address, operational status, MTU, and speed.	*Device Health* For details about the Device Health monitoring policy, see Device Health Monitoring Policy, on page 949.	NA

Network Summary Reports

This section lists the Network Summary reports supported by Cisco Evolved Programmable Network Manager. These reports provide information about the health of the network.

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Polled
Link Flap Report	Tabular representation of the A end device, A end interface, Z end device, Z end interface, link name and the number of flaps.	NA	NA

Optical Performance Reports

Table 15: Optical Performance Reports lists the Optical Performance reports supported by Cisco EPN Manager. For all graphical reports, ensure that you select a maximum of four interfaces while you schedule or run these reports. For all tabular reports, use the Show field to specify the number of records to be displayed in a page while you schedule or run these reports.

The performance data displayed in the generated reports depends on the monitoring policy parameter that you activate when you enable the monitoring policy. For a detailed list of monitoring type and the associated performance counters, see Monitoring Policies Reference, on page 949. For more information about monitoring policies, see Monitor Device and Network Health and Performance, on page 223. For information about how to interpret the report results, see Report Output Examples: Web GUI Output and CSV File Output, on page 307.

Note Enable the *Optical 1 day*, *Optical 15 mins*, or *Optical 30 secs* monitoring policies to populate data for these reports.

Table 15: Optical Performance Reports

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
Ethernet	Ethernet Reports–IOS-XR and SVO devices	Graphical and tabular reports that list the total number of packets that are requested by the higher-level protocols to be transmitted, and which were not addressed to a multicast or broadcast address at this sublayer, including those that were discarded or not sent. The details also include the total number of multicast frames transmitted error free, the total number of packets requested by higher-level protocols, the total number of transmitted octets, the total number of octets received on the interface, and the number of received packets that were discarded because of errors. To customize the report output for a new report, choose **Reports** > **Report Launch Pad** > **Optical Performance** > **Ethernet**. Click **Generate New** and click the **Customize Data** tab. To customize the report output for an existing report, choose **Reports** > **Report Launch Pad** > **Optical Performance** > **Ethernet**, click the required report link, and click the **Customize Data** tab.	*Optical 1 day*, *Optical 15 mins*, or *Optical 30 secs* For details about the information collected by optical monitoring policies, see Monitoring Policies Reference, on page 949. For information about how to interpret the report results, see Report Output Examples: Web GUI Output and CSV File Output, on page 307.	Ethernet

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
OTN	Section Monitoring NEnd & FEnd Reports- Cisco NCS 1000 series, Cisco NCS 2000 series, and Cisco NCS 4000 series devices	Graphical and tabular reports that list the OTN section monitoring details of devices and interfaces in the OTN circuit type. The details include number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, and number of failure counts.	*Optical 1 day*, *Optical 15 mins*, or *Optical 30 secs* For details about the information collected by optical monitoring policies, see Monitoring Policies Reference, on page 949. For information about how to interpret the report results, see Report Output Examples: Web GUI Output and CSV File Output, on page 307.	OTN DWDM Infrastructure[1]
	Path Monitoring NEnd & FEnd Reports	Graphical and tabular reports that list the OTN path monitoring details of devices and interfaces in OTN circuit type. They provide details such as number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, and number of failure counts.		
	Forward Error Correction Reports- Cisco NCS 1000 series, Cisco NCS 2000 series, and Cisco NCS 4000 series devices	Graphical and tabular reports that list the OTN forward error correction details of devices and interfaces in the OTN circuit type. The details include ECW, UCW, the number of bit errors that are corrected, number of uncorrectable words, and preforward error correction-based bit error counts detected during the performance monitoring time interval.		
	Tandem Connection Monitoring NEnd & FEnd Reports	Graphical and tabular reports that provide the tandem connection monitoring details for the devices and interfaces in the OTN circuit type. The details include number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, and number of failure counts.		OTN
	GFP Statistics Reports–Cisco NCS 2000 series and Cisco NCS 4000 series devices	Graphical and tabular reports that provide the Generic Framing Procedure (GFP) statistics for the devices in the OTN circuit type. The GFP statistics include number of GFP frames and bytes received and transmitted, number of single and multiple bit errors received, number of packets received with CRC errors, invalid GFP type, invalid CID, number of CMF frames received and transmitted, and number of cHEC and tHEC multiple bit errors.		OTN DWDM Infrastructure[1]

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
Physical	Optical Power Reports-Cisco NCS 1000 series, Cisco NCS 2000 series, SVO, Cisco NCS 4000 series, Cisco NCS 1010 devices	Graphical and tabular reports that provide the average, minimum, and maximum percentage of optical input and output power of the received and transmitted signal for devices in a physical circuit type. **Note** Graphical reports are not supported for SVO devices.	*Optical 1 day*, *Optical 15 mins*, or *Optical 30 secs* For details about the information collected by optical monitoring policies, see Monitoring Policies Reference, on page 949. For information about how to interpret the report results, see Report Output Examples: Web GUI Output and CSV File Output, on page 307. **Note** *Optical 30 secs* is not applicable for SVO devices	Physical DWDM Infrastructure[1]
	Laser Bias Current Reports- Cisco NCS 1000 series, Cisco NCS 2000 series, SVO, and Cisco NCS 4000 series devices	Graphical and tabular reports that provide the average, minimum, and maximum percentage of laser bias current. The laser bias current is the normalized value expressed as the integer percentage. **Note** Graphical reports are not supported for SVO devices.		
	Optical Physical Report -Cisco NCS 1000 series, Cisco NCS 2000 series, SVO, Cisco NCS 4000 series, Cisco NCS 1010 devices	Graphical and tabular reports that provide the average, minimum, and maximum value of optical power on the unidirectional port. The details include the average, minimum, and maximum Optical Service Channel power level. The details of average, minimum and maximum optical signal-to-noise ratio, optical power warning, chromatic dispersion, second order polarization mode dispersion, polarization dependent loss, differential group delay, polarization change rate, and phase noise. **Note** Graphical reports are not supported for SVO devices.		

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
SDH Or SONET	SDH Regenerator Section Report	Graphical and tabular reports that provide the performance monitoring details of the SDH regenerator section layer for the devices in your network. The details include the number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, number of errored blocks, and number of out-of-frame seconds.	*Optical 1 day* or *Optical 15 mins* For details about the information collected by optical monitoring policies, see Monitoring Policies Reference, on page 949. For information about how to interpret the report results, see Report Output Examples: Web GUI Output and CSV File Output, on page 307.	SDH/SONET DWDM Infrastructure[1]
	SDH Multiplex Section NEnd & FEnd Reports - Cisco NCS 2000 series devices	Graphical and tabular reports that provide the performance monitoring details of SDH multiplex section layer for the devices in your network. The details include number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, number of errored blocks, number of failure counts, protection switching—Switching count, ring count, span count, working count, duration, ring duration, span duration, and working duration.		
	SDH Multiplex Section NEnd & FEnd Reports - Cisco NCS 4000 series devices	Graphical and tabular reports that provide the performance monitoring details of SDH multiplex section layer for the devices in your network. The details include number of background block errors and its ratio, number of errored seconds and its ratio, number of severely errored seconds and its ratio, number of unavailable seconds, and number of errored blocks.		
	SONET Section Report	Graphical and tabular reports that provide performance monitoring details of SONET section layer for the devices in your network. The details include number of coding violations, number of errored seconds, number of severely errored seconds, and number severely errored frame seconds.		
	SONET Line NEnd & FEnd Reports - Cisco NCS 2000 series devices	Graphical and tabular reports that provide performance monitoring details of SONET line layer for the devices in your network. The details include number of coding violations, number of errored seconds, number of severely errored seconds, number of unavailable seconds, number of failure counts, protection switching—Switching count, ring count, span count, working count, duration, ring duration, span duration, and working duration.		

Report	Report Type	Provides:	Monitoring Policy Parameters That Must Be Activated	Parameters That Must Be Polled
	SONET Line NEnd & FEnd Reports - Cisco NCS 4000 series devices	Graphical and tabular reports that provide performance monitoring details of SONET line layer for the devices in your network. The details include number of coding violations, number of errored seconds, number of severely errored seconds, number of unavailable seconds, and number of failure counts.		

1. You must activate this parameter for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices.

Performance Reports

This section lists the basic performance reports supported by Cisco EPN Manager. It also lists the monitoring policies and parameters that must be enabled for each of the report type. These reports are applicable for Optical and Carrier Ethernet technologies.

Note Report types marked with an asterisk (*) are applicable for SVO and Cisco NCS 2000 series devices.

For more information about monitoring policies, see Monitor Device and Network Health and Performance, on page 223.

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Activated
Environmental Temperature	Tabular representation of Device IP Address, name, Sensor Name, Sensor Type, Maximum Inlet Temp, Maximum Other Temp, and Event time for network devices.	*Device Health* For details about the Device Health monitoring policy, see Device Health Monitoring Policy, on page 949.	Environment Temperature
Threshold Violations	Lists the threshold violation alarms data (source, event type, category, and description) for your network in a table.	*Device Health* For details about the Device Health monitoring policy, see Device Health Monitoring Policy, on page 949.	Admin Status Up/Down Operational Status Up/Down Admin Status Up and Operational Status Down Percentage

System Monitoring Reports

This section lists the System Monitoring reports supported by Cisco Evolved Programmable Network Manager. These reports provide information about CPU, Disk and Memory utilization of the network when they exceed threhold limits.

Report Type	Provides:	Monitoring Policies That Must Be Enabled	Parameters That Must Be Polled
CPU Threshold Breach	CPU Utilization for devices in a network. .	NA	NA
Disk Threshold Breach	Disk utilization results when it exceeds the threshold limit.	NA	NA
Memory Threshold Breach	Includes memory utilization results when memory utilization exceeds the threshold limit.	NA	NA

Configure a SFTP Repository

You can configure an external SFTP repository (local or remote) to which you can export reports.

Step 1 Navigate to **Administration** > **Settings** > **System Settings** > **General** > **Report.**

Step 2 Enter details of the SFTP sever in the fields listed under the **External Server Settings** area.

Step 3 Click **Save**.

Create, Schedule, and Run a New Report

The **Report Launch Pad** provides access to all Cisco EPN Manager reports from a single page. From this page, you can perform all report operations: Create, save, view, schedule, and customize.

To see more report details, hover the cursor over the template widget.

To create, schedule, and run a new report:

Before you begin

Ensure that you have configured an external server if you are planning on exporting the report to an external SFTP repository. See Configure a SFTP Repository, on page 302 for more information.

When you run multiple reports, maintain an adequate time interval between the reports which contain huge tables. This avoids overlapping while fetching data.

Step 1 From the left sidebar, choose **Reports** > **Reports** > **Report Launch Pad**, and choose **Templates**.

Step 2 Locate the report that you want to launch (you can filter the reports by checking/unchecking the checkboxes based on the report type under the **Refine & Filer** pane), and click **Generate New**.

Step 3 Under the **Report Details** window, enter the report title.

You can edit the **Report Title** field.

Step 4 Choose the appropriate **Report By** category from the drop-down list.

Step 5 The **Report Criteria** field allows you to sort your results depending on the previous **Report By** selection made.

Note If you select the virtual domain checkbox at the top, edit button is enabled when one or more values present in the report criteria filter.

Step 6 Select the values from **Severities** and **Categories** drop-downs. Choose the **Reporting Period**.

Step 7 If you plan to run this report later or as a recurring report, click the **Export and Schedule** tab, click the **Export** slider, and choose the report type. Select the report export file format (CSV, XML, HTML, or PDF). Exported CSV file is a single .csv file, which has capability to hold one million records. If the number of records exceeds one million, then another CSV file will be generated accommodating the remaining records. Finally, the CSV files are generated in a zip format. Select one of the **Destination** options (File, Email, or SFTP).

Step 8 Check the **Schedule** slider, and choose the date and time to run the report.

Step 9 To run the report, choose one of the following options:

- **Run**—runs the report without saving the report setup.
- **Save**—

  If you have not saved any parameters, the report is saved without running it.

  If you have enabled the **Export** option and enetered related details, the report is saved and is run immediately.

  If you have enabled both the **Export**and **Schedule** options and entered related details, then the report is saved and is run at the scheduled date and time that you have entered.
- **Cancel**—returns to the previous page without running or saving this report.

Customize Report Results

Many reports allow you to customize their results, letting you include or exclude different types of information. Reports that support this feature display a Customize button. Click this button to access the Create Custom Report page and customize the report results.

To customize a report result:

Step 1 Click **Reports > Reports** > **Generated Reports** and, then select the report that you want to customize. Click the **Edit** icon.

Step 2 In the **Edit Report** page, click the **Customize Data** tab and complete the required information. You can choose report columns as well as sort the reports based on different criteria.

Step 3 Click **Save** to save the changes.

Filter and Customize Report Data Using User Defined Fields

You can create custom attributes and assign values to them. See Create User Defined Fields for Custom Values, on page 110 for information about how to create user defined fields (UDF). You can then use the UDFs to filter and customize the report results.

Cisco Evolved Programmable Network Manager scans the values of UDFs created every two minutes and generates a UDF.json file, in which the metadata are saved. You can access this file from the `/opt/CSCOlumos/conf/rfm/classes/com/cisco/server/reports/conf/UDF.json` location.

Here is an example of how the metadata for the UDFs are displayed in the UDF.json file:

```
[
  {
    "label": "internal",
    "hidden": true,
    "displayName": "Internal",
    "fixedColumn": false
  },
  {
    "label": "location",
    "hidden": true,
    "displayName": "Location",
    "fixedColumn": false
  },
  {
    "label": "quality",
    "hidden": true,
    "displayName": "Quality",
    "fixedColumn": false
  },
```

In this example:

- the attribute, *label* is the user defined field created in the **Administration** > **Settings** > **System Settings** > **General** > **User Defined Fields** page.
- the attribute, *hidden* is set to False, by default. If this attribute is set to True, the UDF is hidden on the Reports page. You need to set this attribute to False so that the UDF is available for selection when you customize the report results.
- the attribute, *displayName* is used to change the UDF name that will be displayed in the report results.
- The attribute, *fixedColumn* is applicable only when the hidden attribute is set to False.

After you have made the required changes in the UDF.json file, you can customize the report results. See Customize Report Results, on page 303.

You can filter and customize reports based on UDFs for the following reports:

Report Category	Report Name	Report Type
CE Performance	Interface Graphs	Interface In Utilization Graph
		Interface In Traffic Graph
		Interface Out Utilization Graph
		Interface Out Traffic Graph
	Interface Top N	Interface TopN In Utilization
		Interface TopN In Traffic
		Interface TopN Out Utilization
		Interface TopN Out Traffic
		Interface Bottom N Availability
	Interface Traffic	Interface Errors and Discards
		Interface Traffic Report
		Interface CRC Errors Report
Performance	Environmental Temperature	Summarized Environmental Temperature
		Current Environmental Temperature
Device	CPU Utilization	CPU Utilization
		Top CPU Utilization
		Bottom CPU Utilization
	Memory Utilization	Memory Utilization
		Top Memory Utilization
		Bottom Memory Utilization
	Wired Module Detail	Wired Module Detail Report Details
	Wired Detailed Device Inventory	Wired Detailed Device Inventory Report Details

You can also change the filter type of the UDF in the UDF.json file. The default filter type is String.

Here are few examples of filter types and their definitions:

```
[
  {
    "label": "internal",
    "displayName": "Internal",
```

```
    "hidden": false,
    "fixedColumn": false,
    "filterMetadata": {
      "sqlDataType": "Boolean",
      "attr": "internal",
      "label": "UDF: Internal Used",
      "filterType": "boolean"
    }
  },
  {
    "label": "location",
    "displayName": "Location",
    "hidden": false,
    "fixedColumn": false
  },
  {
    "label": "quality",
    "displayName": "Quality",
    "hidden": false,
    "fixedColumn": false,
    "filterMetadata": {
      "sqlDataType": "Number",
      "selectItems": {
        "1": "High Quality",
        "2": "Mid Quality",
        "3": "Low Quality"
      },
      "attr": "quality",
      "label": "UDF: Quality",
      "filterType": "enumeration"
    }
  },
  {
    "label": "sapid",
    "displayName": "SAP ID",
    "hidden": false,
    "fixedColumn": true,
    "filterMetadata": {
      "sqlDataType": "Number",
      "attr": "sapid",
      "label": "UDF: SAP ID",
      "filterType": "numeric"
    }
  },
  {
    "label": "startTime",
    "displayName": "Start Time",
    "hidden": false,
    "fixedColumn": false,
    "filterMetadata": {
      "sqlDataType": "Timestamp",
      "attr": "startTime",
      "label": "UDF: Start Time",
      "filterType": "datetime"
    }
  },
  {
    "label": "vendor",
    "displayName": "Vendor",
    "hidden": false,
    "fixedColumn": true,
    "filterMetadata": {
      "sqlDataType": "String",
      "selectItems": {
```

```
        "huawei": "Hua Wei",
        "alu": "Alcatel Lucent",
        "cisco": "Cisco"
      },
      "attr": "vendor",
      "label": "UDF: Vendor",
      "filterType": "enumeration"
    }
  }
]
```

After you have made the required changes in the UDF.json file, use the **Advanced Filter** option in the Report Details page to filter the report data.

Report Output Examples: Web GUI Output and CSV File Output

In this example, a section monitoring report is generated for Cisco NCS 2000 series devices that are available in the near end of the network. You can choose to view the result, either at the bottom of the Report Details page, or export the results in CSV, XML, HTML, or PDF format files. For more information on how to create and run a report, see Create, Schedule, and Run a New Report, on page 302.

If scheduling is enabled and you choose to export the result to a CSV file, the report is saved in the repository named as /localdisk/ftp/reports. You can adjust the location of the report repository. For more information, see Report Purging, on page 787.

Note If scheduling is disabled and you choose to export the result to a CSV file, the report is saved in the repository named as /localdisk/ftp/reportsOnDemand.

The file naming convention for the CSV file is *ReportTitle_yyyymmdd_hhmmss*.csv, where *yyyymmdd* is the year, month, and date, and *hhmmss* is the hours, minutes, and seconds when the report result is exported.

The following figure shows how the results are displayed in a CSV file.

	A	B	C	D	E	F	G	H	I	J	K	L
1	Section Monitoring Report for Cisco NCS 2000 Series Devices											
2	Generated: 20 17:52:03 IST											
3	Report By: Interfaces By Device											
4	Devices: M6-235-140;nmtgte-m6-159;M6-235-139											
5	Report Interval: 15 minutes											
6	Reporting Period: Last 6 hours											
7	Show: All records											
8												
9	Section Monitoring NEnd Report											
10	Device Name	Device IP Address	Interface	DateTime	BBE-SM	BBER-SM	ES-SM	ESR-SM	SES-SM	SESR-SM	UAS-SM	FC-SM
11	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:00:00 IST	0	0	0	0	0	0	0	0
12	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:15:00 IST	0	0	0	0	0	0	0	0
13	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 12:30:00 IST	0	0	0	0	0	0	0	0
14	M6-235-140	10.58.235.140	CHAN-2-2-2	2015-Apr-02, 13:00:00 IST	0	0	0	0	0	0	0	0

403224

The following table explains how you can interpret the section monitoring report result.

Column Name	Description
Device Name	Name of the device that is in the near end of the network.
Device IP Address	IP address of the device.

Column Name	Description
Interface	Interface name of the device.
Date/Time	Date and time when the section monitoring data was collected for the device. The value in this column depends on the report interval that you chose when you created the report. The report interval can be 15 minutes or 24 hours.
BBE-SM	Number of background block errors for the device.
BBER-SM	Background block error ratio for the device.
ES-SM	Number of errored seconds for the device.
ESR-SM	Errored seconds ratio for the device.
SES-SM	Number of severely errored seconds for the device.
SESR-SM	Severely errored seconds ratio for the device.
UAS-SM	Number of unavailable seconds for the device.
FC-SM	Number of failure counts (AIS/RFI detected) for the device.

For detailed descriptions of performance counters that are displayed in the results of other optical performance reports, see Performance Counters for Optical Monitoring Policies, on page 958.

Troubleshooting Tips for an Empty Report

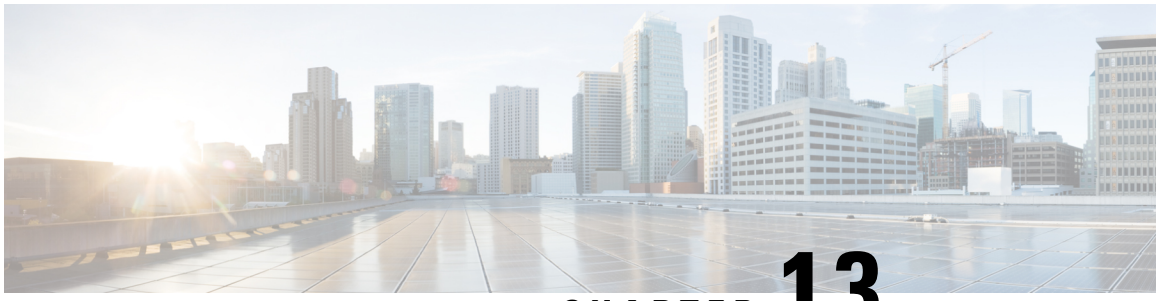
If the report was run successfully but you do not have an output file that can be exported, you can try one of the following troubleshooting tips:

Check if you have...	For example:
...enabled the correct monitoring policy. For details on what monitoring policies must be enabled, see Monitoring Policies Reference, on page 949.	For QoS reports, QoS monitoring policy must be enabled.
... enabled the periodic collection.	For any System Monitoring Periodic reports (CPU/Disk/Memory), the periodic collection must be enabled. Once enabled, the report must be generated after 12 hours to see the output. **Note** To enable Periodic collection, • Visit link: `https://<Server IP>/webacs/ncsDiag.jsp` • Select **Monitoring Settings**, and click the **Periodic Collection Enable** button.

Check if you have...	For example:
... chosen the correct device type for a particular report.	Do not choose NCS devices for generating CE Performance reports as they are optical devices.
... selected the correct time period while generating a report.	You cannot choose a 2-week time period if you enabled the policy only two days ago.
... configured the device properly. For more details, see Configure Devices So They Can Be Modeled and Monitored, on page 53.	For QoS reports, QoS must be configured/enabled on the device.
... successful device inventory collection. For more details, see Find Devices With Inventory Collection or Discovery Problems, on page 70	For the reports to have data, the inventory collection status must be **Completed**.

PART V

Configure Devices



CHAPTER 13

Configure Devices

This chapter provides the following topics:

Ways to Configure Devices Using Cisco Evolved Programmable Network Manager

Cisco EPN Manager provides two ways to change the physical devices in your network. The actions you can perform depend on your user account privileges and the types of devices in your network.

Launch Points for Configuring Devices	Use this method to:
Configuration menu from left-side navigation menu	Click on a **Device Name**, then click the **Configuration** tab. You can configure device features on the selected device. You can also view the list of applied and scheduled feature templates that were deployed to the device.
Create and deploy configuration templates	Perform common network management tasks on *one or more devices* using system templates—for example, adding a hostname or configuring a routing protocol. You can also create your own templates to fit your deployment needs. Because they can be applied to multiple devices, templates normally apply to specific device operating systems or device types. When you use a configuration template, Cisco EPN Manager only displays devices that meet the template criteria.

Note You can also edit device properties from the Network Devices table (**Configuration** > **Network** > **Network Devices**) by choosing a device and clicking **Edit**. This launches the Edit Device wizard. However, changes you make using the wizard are limited to device credentials, and any changes you make do not affect the physical device; they only update device information that is stored in the database.

For optical devices, you can also configure devices using Cisco Transport Controller, which you can launch from Cisco EPN Manager. See Launch Cisco Transport Controller to Manage Cisco NCS and Cisco ONS Devices, on page 450

After you make your changes, save your changes to the database and optionally collect the device's physical and logical inventory. For more information, see Collect a Device's Inventory Now (Sync), on page 449.

Which Devices Support the Configuration Operations?

Configuration operations are supported on a device if:

- The device model is supported by Cisco EPN Manager.
- The device operating system is supported by Cisco EPN Manager.
- The applicable technology or service is supported by Cisco EPN Manager *and* is enabled on the device.

To find out what is supported, see Cisco Evolved Programmable Network Manager Supported Devices.

Identify the Commands Used In a CLI Configuration Template

Use this procedure to view the exact commands that are used by any of the commands you launch from the **CLI Templates** drawer.

Step 1 Choose **Configuration** > **Templates** > **Features and Technologies** > **CLI Template** > **CLI** , then choose **s**. For example:

- Out-of-the-box templates are under **System Templates - CLI**.
- Customized templates are under **My Templates**.

Step 2 Double-click the template in the left sidebar **Templates** menu.

Step 3 In the Template Detail area, choose the **CLI Content** tab. The commands are displayed in that tab.

Change a Device's Credentials and Protocol Settings

Use the following procedure to update device credentials and protocol settings. When you save the settings to the database, you can also perform an inventory collection to gather all physical and logical device changes and save those changes to the database, rather than wait for the daily inventory collection.

Step 1 Choose **Inventory** > **Network Devices**.

Step 2 Select the device you want to edit, and click **Edit**. You can also choose several devices and make bulk changes.

Step 3 Double-click the parameters you want to change. Depending on the device type, you can edit:

- Credential profile being used by device
- Group the device belongs to
- SNMP port, retries, timeout, credentials, and SNMPv3 authentication information
- Telnet/SSH credentials and timeout
- HTTP/HTTPS credentials, port, timeout
- TL1 credentials and proxy IP address (for GNE/ENEs)
- Civic Location

Step 4 Check that the new credentials are the same as those on the physical device by clicking **Verify Credentials**.

Step 5 Save your changes:

- **Update** saves your changes in the database.
- **Update & Sync** saves your changes to the database, but also collects device physical and logical inventory and saves all changes to the database.

Change Basic Device Properties

Cisco EPN Manager provides command templates that you can use to make basic property changes on your physical devices.

To use these templates, choose **Configuration** > **Templates** > **Features & Technologies**, then choose **CLI Templates** > **System Templates – CLI** from the Templates pane on the left.

Note The operations you perform here are different from those you perform with the Edit wizard (which you can launch from the Network Devices table). The Edit wizard changes the device property information that is saved in the database. It does not change properties on physical devices.

CLI Configuration Template Name	Use it to:	Required Input Values
Add-Host-Name-IOS *and* -IOS-XR	Configure the client host name	Host name
Remove-Host-Name-IOS *and* -IOS-XR		
Syslog-Host-Logging-IOS and -IOS-XR	Specify host to which messages of a certain level will be logged	Host name
Add-Tacacs-Server-IOS *and* -IOS-XR	Configure the TACACS or TACACS+ server to use for authentication	Host address, key value, authentication list name, group name
Remove-Tacacs-Server-IOS *and* -IOS-XR		
Add-Tacacs-Plus-Server-IOS *and* -IOS-XR		
Remove-Tacacs-Plus-Server-IOS *and* -IOS-XR		
Add-SNMP-Configuration-IOS *and* -IOS-XR	Configure SNMP version, password, password encryption, server and group settings, UDP port, and so forth	Host name, community name, SystemOwner
Remove-SNMP-Configuration-IOS *and* -IOS-XR		
Enable-Traps-ASR903	Enable and disable traps on the Cisco ASR 903	Trap name (a list is provided)
Disable-Traps-ASR903		
Enable-Traps-IOS *and* -IOS-XR	Enable and disable traps on Cisco IOS and Cisco IOS-XR devices	
Disable-Traps-IOS *and* -IOS-XR		
Enable-Trap-Host-IOS *and* IOS-XR	Set a target host for SNMP traps	Host IP address, community string
Show-Users-on-Device-IOS and -IOS-XR	Display user session information for Cisco IOS and Cisco IOS XR devices	(Executed from selected device; no input required)

Enable and Disable Interfaces

Use the Interface 360 view to quickly enable and disable an interface. While you can perform these same actions from a Device Details page, using the Interface 360 view may be more efficient (for example, when

responding to an alarm). The top right of the Interface 360 view provides an **Actions** menu that provides enable and disable options.

To launch an Interface 360 view, see Get a Quick Look at a Device Interface: Interface 360 View, on page 103.

To enable and disable an interface from a device's Device Details page, see the interface configuration topics (Ethernet, Loopback, Serial, Tunnel, and so forth).

Configure Physical Attributes of Device Interfaces

Using Cisco EPN Manager, you can configure the physical attributes of your device's interfaces. Attributes such as card operating modes, bandwidth allocation per slot, slot pluggable types (such as VCoP), and AINS settings are configurable.

To configure the physical attributes of interfaces:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device's name hyperlink.

Step 3 Click the **Device Details** tab.

Step 4 To configure the interfaces, navigate to the paths described in the table below.

Step 5 To make your changes, click the controller/card name hyperlink and click the Edit icon at the top-right corner of the page. Make your changes and click **Save**.

Table 16: Physical Attributes Configuration for Interfaces

Physical Interface Configuration	Navigation	Comments/Descriptions	Supported Slots/Controllers
Configure card type as 5G or 10G.	**Physical** > **Card Mode**	You can change the configuration from 10G to 5G but the other way around is not supported. Depending on the device you select, the default card mode is set to either 5G or 10G. For mode detailed information on the supported card modes, see Supported Devices for Cisco EPN Manager **Note** You cannot configure the card modes on slots that are part of active circuits.	For more information about the device slots and supported card mode types, see table below (*Device Slots and Supported Card Mode Types*).
Configure card modes as T1 or E1.	**Physical** > **Card Mode**	You can change the configuration from T1 to E1 or conversely depending on the device and card you select. T1 and E1 modes represent the type of channelization mode used on the card. **Note** You cannot configure the card modes on slots that are part of active circuits.	-

Physical Interface Configuration	Navigation	Comments/Descriptions	Supported Slots/Controllers
Configure card modes as OC3 or OC12.	**Physical** > **Card Mode**	You can set the card modes of A900-IMA4OS cards (of Cisco ASR 903 routers) as OC3 or OC12. OC3 and OC12 modes represent the data transmission rates on the different optical transmission lines.	-
Configure Card Protection	**Physical** > **Card Protection**	Configure cards to act as primary or backup members (interfaces). A primary interface and its backup interface together make up a Protection Group (denoted by a unique integer). Associating cards with backup members ensures that when the primary interface fails, the protecting interface quickly assumes the traffic load from the primary interface. Cards displayed as the Active members are cards functioning as the protecting members of the service. Ensure that the Primary and Backup members are of the same type. For example, if you choose a T1 interface as a Primary member, the Backup member must also be a T1 interface. Hold-Off Timer is available for 1+1 card protection (NCS 42XX devices having IOS-XE version 16.10.1 or higher). It is used to prevent the successive switching in case of network inconsistency. The valid range is 0–10 seconds. Default value is 5. The Admin Mode for the protection group is configured in the order Lockout > Force Switch > Manual Switch > None. For more information about these modes and the revert timer, see the descriptions in Configure APS or MSP and UPSR or SNCP Protection Groups, on page 327.	-
Configure NCS4200-1T16G-PS cards on NCS42xx devices.	**Physical** > **Card Mode**	You can view all the card modes of NCS4200-1T16G-PS cards, irrespective of the slot numbers. **Note** Once you configure NCS4200-1T16G-PS card on some slots of NCS42xx devices, the configurations on those slots will be reset to the default values.	-
Configure A900-IMA8CT1Z-M and A900-IMA8CS1Z-M cards on ASR9xx devices.	**Physical** > **Card Mode**	You can view and configure the card modes of A900-IMA8CT1Z-M and A900-IMA8CS1Z-M cards.	-

Physical Interface Configuration	Navigation	Comments/Descriptions	Supported Slots/Controllers
Configure the interface module type for Automatic In-Service (AINS)	**Physical** > **Automatic In-Service (AINS)**	Use the **Cards** tab to configure the right controller types for AINS. In case of manual insertion and removal of cards, the AINS values are populated after a 20 min delay. The ports/controllers tabs list all the AINS enabled ports and controllers. The supported ports and controllers are: Ethernet, E1, E3, T1, T3, and SONET SDH and STS1E. You can use the Edit icon to set the Secondary Admin State and Soak Timer (in hours or in minutes) values. **Note:** Enabling AINS on a port/controller is an operation to be performed on the device manually. Following are the Secondary Admin State values that you can set: • IS_AINS—indicates that the device is in Automatic In-Service state. • IS—indicates that the device is in in-service state. • OOS_MT—indicates that the device is in maintenance state. Use the **Soak Timer Hours** field to set the soak timer in hours. The valid range is 0-48 hours. Use the **Soak Timer Minutes** drop-down list to set the soak timer in minutes. The available values are: 15, 30, and 45 minutes. The default value is 15 minutes.	-
Configure bandwidth that must be reserved for the selected device slots.	**Physical** > **Bandwidth**	The bandwidth you specify is reserved for the selected slot and made available to the slot irrespective of whether the slot is operational or not. In cases when the selected slot/card is down, and then back online after sometime, the configured bandwidth will be available for use based on the values specified in this field.	You can reserve a preconfigured bandwidth value of 80 Gbps or 100 Gbps on NCS4200-1T16G-PS cards on NCS4216 devices.
Configure the interface pluggable type for virtual Container over Packet (VCoP).	**Physical** > **Pluggable Type**	Use this menu to select the right port types for VCoP enabled interfaces. For example, the port types can be OC3, OC12, or DS3. **Note** VCoP smart SFP provides an ability to forward the SONET signal transparently across the packet network. The VCoP smart SFP is a special type of optical transceiver which encapsulates SONET bit stream at STS1 or STS-3c or STS-12c level into packet format.	-

Conditions and Limitations: Following are the conditions and limitations for configuring controller modes on Cisco ASR 900 Series Route Switch Processor 2 (RSP2A) modules (A900-RSP2A-128) that are supported on Cisco ASR 920, Cisco NCS4202, and Cisco NCS 4206 devices:

- The maximum bandwidth that can be configured is OC-48. A maximum of 20 ports on the module can be configured:
  - Ports 0-11 are T1 ports.
  - Ports 12-15 are T3/E3 ports.
  - Ports 16-19 are OC3/OC12 ports.

  Note If a given port is configured as OC48, then only one of the given ports can be configured since the maximum configurable bandwidth is OC48.

- Configuration limitations on the Cisco A900-RSP2A-128 modules:
  - You cannot configure SDH/E3/E1/DS0 controller modes.
  - Configuring Ethernet as the controller mode is not supported.
  - The protection type UPSR cannot be configured.
  - Once you deploy the controller mode configuration to the device, you cannot undo the configuration using Cisco EPN Manager.

Table 17: Device Slots and Supported Card Mode Types

Cisco NCS 4206 Devices	Cisco NCS 4216 Devices	Cisco ASR903 Devices	Cisco ASR907 Devices
• Slot 0, 1 - Not supported • Slot 2, 3, 4, 5 - Default Mode 10G	• Slot 0, 1 - Not supported • Slot 3, 4, 7, 8, 11, and 12 - Default Mode 10G • Slot 2, 5, 6, 9, 10, 13, 14 and 15 - Default Mode 5G	• Slot 0, 1 - Not supported • Slot 2, 3, 4, 5 - Default Mode 10G	• Slot 0, 1 - Not supported • Slot 3, 4, 7, 8, 11, and 12 - Default Mode 10G • Slot 2, 5, 6, 9, 10, 13, 14 and 15 - Default Mode 5G

Table 18: Controller Modes and Supported Port Types

SONET (0-3)	SONET (4-7)
• Max of 2.5G • Can support OC48/OC12/OC3 but total of 2.5G • Example if Port 0 configured with OC48, Port1/2/3 can't be used	• Max of 2.5G • If a port group has OC12/OC3/1G, it means OC48 can't be allowed

Configure Circuit Emulation

Cisco EPN Manager supports the provisioning of Circuit Emulation (CEM) which provides a bridge between traditional TDM network and packet switched network (PSN). CEM is a way to carry TDM (or PDH) circuits over packet switched network. Circuit Emulation (CEM) is the imitation of a physical connection. This feature allows you to use your existing IP network to provide leased-line emulation services or to carry data streams or protocols that do not meet the format requirements of other multiservice platform interfaces.

Cisco EPN Manager supports the following CEM modes:

- Structure-Agnostic time-division multiplexing (TDM) over Packet (SAToP)—This is the unstructured mode in which the incoming TDM data is considered as an arbitrary bit stream. It disregards any structure that may be imposed on the bit stream. SAToP encapsulates the TDM bit streams as pseudowire (PWs) over PSN.
- Circuit Emulation over Packet (CEP)—This mode is used to emulate Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) circuits and services over MPLS. To transport SONET/SDH circuits through a packet-oriented network, the Synchronous Payload Envelope (SPE) or Virtual Tributary (VT) is broken into fragments. A CEP header and optionally an RTP header are prepended to each fragment.

For more information about CEM in Cisco EPN Manager, see, Supported Circuit Emulation Services, on page 492.

When a line is channelized, it is logically divided into smaller bandwidth channels called higher-order paths (HOP) and lower-order paths (LOP). These paths carry the SONET payload. When a line is not channelized, the full bandwidth of the line is dedicated to a single channel that carries broadband services. Cisco EPN Manager enables you to channelize the T3 or E3 channels into T1s, and channelize the T1s further into DS0 time slots. Before you provision CEM services using Cisco EPN Manager, you must first configure the parameters for the HOP and LOP by configuring the interfaces for CEM.

A channelized SONET interface is a composite of STS streams, which are maintained as independent frames with unique payload pointers. The frames are multiplexed before transmission. SONET uses Synchronous Transport Signal (STS) framing while SDH uses Synchronous Transport Mode (STM) framing. An STS is the electrical equivalent to an optical carrier 1 (OC-1) and an STM-1 is the electrical equivalent to 3 optical carrier 1s (OC-1s).

This section describes how you can use Cisco EPN Manager to first configure your interfaces for CEM. You can then provision CEM services using these interfaces configured with appropriate controller modes and protection groups.

Pre-requisites for Configuring CEM Services

Before you provision a CEM service (see Provision Circuit Emulation Services, on page 573), ensure that the following pre-requisites are met:

- Configure the required loopback settings for CEM on the device. See, Configure Loopback Interfaces, on page 351.
- Configure the required CEM parameters on SONET, SDH, PDH, HOP, and HOP controllers. See, Configure Interfaces for CEM, on page 323.

- Configure the working and backup interface groups to provide APS protection. See, Configure APS or MSP and UPSR or SNCP Protection Groups, on page 327.

SONET Modes Configuration Examples

The following configuration commands and examples shows how to configure STS-1 modes.

Configure STS-1 Modes

To configure STS-1 modes, use the following commands:

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
mode vt-15
end
```

Note There is no default mode. The modes vt-15, mode ct3, mode t3, mode unframed, mode vt-2 are supported. To restore the system to its default condition, use the **no** form of the command.

Configuring DS1/T1 CT3 mode of STS-1:

To configure DS1/T1 CT3 mode of STS-1, you can configure the T1 link using the following steps:

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
mode ct3
t1 1 clock source internal
t1 1 framing unframed
end
```

Note To restore the system to its default condition, use the no form of the command.

Configuring STS-Nc - Contiguous Concatenation

To configure STS-Nc - contiguous concatenation, use the following commands:

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1-3 mode sts-3c
end
```

Note To restore the system to its default condition, use the **no** form of the command. Also, to configure STS-3c or STS-12c, use the numbers as multiples for 3 or 12, respectively.

Configuring CEM Group for Sonet Mode VT1.5-T1 in CESoPSN

To configure CEM group in VT 1.5 mode of STS-1 for CESoPSN, use the following commands

```
enable
configure terminal
controller sonet 0/5/0
sts-1 2
mode vt-15
vtg 1 t1 1 cem-group 56 timeslots 1 - 8
end
```

Configuring CEM Group for Sonet Mode CT3-T1 in CESoPSN

To configure CEM group in CT3 mode of STS-1 for CESoPSN, use the following commands:

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
mode ct3
t1 3 cem-group 28 timeslots 1 - 7
end
```

Configure Interfaces for CEM

Using Cisco EPN Manager, you can configure your interfaces with Circuit Emulation (CEM). To do this, you must set the appropriate controller modes on your interfaces and then configure the PDH (E1, T1, E3, T3), SONET, and SDH controllers for CEM. After you configure the interfaces with CEM, you can then use the interfaces for provisioning CEM services. See Provision Circuit Emulation Services, on page 573.

To configure the interfaces for CEM:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device name hyperlink.

Step 3 Click the **Device Details** tab.

Step 4 To configure CEM parameters, navigate to the configuration options as described in the following table.

Step 5 To make your changes, click the controller/card name hyperlink and click the Edit icon at the top-right corner of the page. Make your changes and click **Save**.

Example

Table 19: CEM Interface Configuration Options

CEM Interface Configuration	Navigation	Comments / Descriptions	Supported Slots/Controllers
Configure controller modes as SONET, SDH, Ethernet, T3, or E1, E3, or STS1E.	**Circuit Emulation** > **Controller Mode**	The controller mode options displayed for selection are based on the selected media type. For details, see Controller Modes and Supported Port Types.	–
Configure PDH (E1, T1, E3, and T3) controllers	**Circuit Emulation** > **PDH**	For a description of the different PDH parameters, see CEM Interface (PDH, SONET, and SDH) Field Descriptions, on page 331	-
Configure SONET and SDH controllers for CEM	**Circuit Emulation** > **SONET and SDH**	For a description of the different SONET and SDH parameters, see CEM Interface (PDH, SONET, and SDH) Field Descriptions, on page 331	For more information about the device ports and supported controller types, see following table (*Controller Modes and Supported Port Types*).

CEM Interface Configuration	Navigation	Comments / Descriptions	Supported Slots/Controllers
Configure a working and protecting member interface for CEM provisioning.	**Circuit Emulation** > **Protection Group**	See Configure APS or MSP and UPSR or SNCP Protection Groups, on page 327	-

Controller Modes and Supported Port Types

- There are pair wise restrictions for EOWYN IM. Valid pairs are (0,1) (2,3) (4,5) (6,7).

Note For each pair, you can configure maximum of 2.5Gbps(OC48) bandwidth(both ports combined).

- You can only configure rates OC3/OC12/OC48 for ports 0-7 and only rate OC192 on port 8.

Table 20: Bandwidth used by different rates OCN -> n * 51.84 Mbit/s

Rate Configuration	Bandwidth
OC1	51.84 Mb/s
OC3	155.52 Mb/s
OC12	622.08 Mb/s
OC48	2488.32 Mb/s ~= 2.5 Gb/s
OC192	9953.28 Mb/s ~= 10 Gb/s

Configure MediaType Controller

To configure MediaType Controller, use the following commands:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
end
```

Configure SONET Ports

To configure SONET ports, use the following commands:

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
```

```
rate OC12
end
```

The earlier example shows how to configure SONET ports in OC-12 mode.

Configure STS1E Ports

To configure STS1E ports, use the following commands:

```
NCS4200-120.33#sh run | sec 0/4/0
controller MediaType 0/4/0
 mode sts1e
controller STS1E 0/4/0
 no snmp trap link-status
 no ais-shut
 alarm-report all
 secondary-admin-state auto-in-service
 clock source internal
 cablelength short
 overhead j0 tx length 64-byte
 overhead j0 expected length 64-byte
 !
 sts-1 1
```

CEM Interface Configuration Example:

- The following example shows the sample CEM interface configuration that is deployed to the device for CEM framing type 'unframed', c-11 mode, clock source of type 'internet', and ACR values associated with the Protection Group 'acr 255':

```
NCS4206-120.32#show running-config | section 0/4/0
controller MediaType 0/4/0
 mode sonet
controller SONET 0/4/0
 rate OC3
 no ais-shut
 framing sonet
 clock source line
 loopback network
 !
 sts-1 1
  clock source internal
  mode unframed
  cem-group 1 cep
 !
 sts-1 2
  clock source internal
  loopback network
  mode unframed
  cem-group 2 cep
 !
 sts-1 3
  clock source internal
  mode vt-15
  vtg 1 vt 1 protection-group 15 working
  vtg 1 vt 3 protection-group 16 working
  vtg 1 vt 4 protection-group 17 working
 !
 aps group acr 255
 aps protect 1 6.6.6.6 / aps working 1
!
interface CEM0/4/0
 no ip address
 cem 1
 !
```

```
 cem 2
 !
connect sam CEM0/4/0 1 CEM0/4/0 2
 !
NCS4206-120.32#
```

- The following example show the sample CEM interface configuration with STS1E.

```
controller STS1E 0/4/1
  sts-1 1
    mode vt-15
    vtg 1 t1 1 cem-group 0 cep
interface CEM0/4/1
 no ip address
 cem 0
 !


controller STS1E 0/4/0
 sts-1 1
  clock source internal
  mode unframed
  cem-group 0 cep
interface CEM0/4/0
 no ip address
 cem 0
 !
```

Configure APS or MSP and UPSR or SNCP Protection Groups

Viewing the protection groups for CEM helps you understand the enabled Automatic Protection Switching (APS), Unidirectional Path Switched Ring (UPSR), Multiplex Service Protection (MSP) and Subnetwork Connection Protection (SNCP) interfaces for your devices. APS and UPSR refer to the mechanism of using a protect interface in the SONET network as the backup for the working interface. Associating your interfaces with APS or UPSR protection groups, ensures that when the working interface fails, the protect interface quickly assumes its traffic load. The working interfaces and their protect interface together make up a Protection Group. SONET Protection Groups offer recovery from fiber (external) or equipment (interface and internal) failures at the SONET line layer. Using Cisco EPN Manager, you can view the working member for a SONET controller which acts as the main functioning controller for the CEM circuit. The Protecting Member acts as a backup for the main working controller. To view these details, ensure that the interfaces have been set with the required controller modes as explained in Configure Interfaces for CEM, on page 323.

MSP and SNCP refer to the mechanism of using a protect interface in the SDH network as the backup for the working interface. Associating your interface with MSP or SNCP protection groups, ensures that when the working interface fails, the protect interface quickly assumes its traffic load. The working interfaces and their protect interface together make up a Protection Groups.

MSP is a protection mechanism in SDH for a port level protection, which provides 1+1 protection mechanism. In network topology map, all modes are supported including revertive, unidirectional, bidirectional, and acr/dcr modes. MSP in SDH is similar to APS in SONET. For example, in NCS 4206 device it has both working and protection modes.

SDH-MSP feature provides port level redundancy for SDH controller across Interface Module (IM). You can configure ports of different IM with one in working mode and the other port in protect mode.

SNCP is a protection mechanism for SDH networks that enables SDH connections to switch to another SDH circuit when a circuit failure occurs. A protection interface serves as the backup interface for the working interface. When the working interface fails the protection interface quickly assumes its traffic load. The switchover to a protection path occurs in the nonrevertive mode. If protection is switched to the protection path due to a transmission fault, there is no automatic switch-back to the original path once the fault is rectified. The functional equivalent of SNCP in SONET is called UPSR. You can provision CEM services and SNCP through Provision wizard or through CLI. The supported modes are VC4_16C, VC4_4C, VC4, AU4_VC12, AU4-VC11, AU3-VC12, AU3-VC11.

Note Mix mode support is not available.

Some Limitations are:

- SDH supported modes with SNCP is not supported on STM64 port.
- LOOPBACK and Bit Error Rate Testing (BERT) can be configured only on physical member controllers.
- The supported scale is limited to 336 circuits.

Before you modify the protection groups ensure to add controllers/interfaces to protection.

To configure APS/MSP protection groups and view UPSR/SNCP interfaces:

Step 1 Choose **Configuration** > **Network Devices**.

Step 2 Select the device that is configured with protection groups, by clicking the device's name hyperlink.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Circuit Emulation** > **Protection Group**.

Step 5 To configure the APS/MSP parameters, click the **APS/MSP** tab, click the Protection Group hyperlink of the group that you want to modify, and click the Edit icon at the top-right corner of the page.

Step 6 You can view and configure the following fields.

- The **Working Member** represents the SONET/SDH controller which acts as the main functioning controller for the circuit.
- The **Protecting Member** represents the SONET /SDH controller which acts as the backup to the working member for the circuit.
- The **Protection Status** indicates whether the group is an active or inactive member for the circuit.
- The **Hello Time** and **Hold Time** fields represent the time range for the protecting and working members. The hello timer defines the time between hello packets. The hold timer sets the time before the protect interface process declares a working interface's router to be down. By default, the hold time is greater than or equal to three times the hello time.
- The **Loopback IP** determines the configuration for the protect interface which includes the IP address of the router (normally its loopback address) that has the working interface.
- The **Revertive Time**, in minutes, enables automatic switchover from the protect interface to the working interface based on the configured time after the working interface becomes available. If revertive time is zero then the protection is non-revertive.
- The **Directional** drop-down menu represents the direction in which the backup protection must be enabled.

- In the bidirectional mode, a failure on a working member triggers an APS/MSP switchover of the working member to the Protecting member. Here the receive and transmit channels are switched as a pair.
- In the unidirectional mode, failure on a working member triggers an APS/MSP switchover of only the failed member to the corresponding line of the Protection interface.

- The **ADM** checkbox, if enabled, associates Add Drop Multiplexers (ADMs) with the protecting member.
- The **APS Request** drop-down menu enables you to configure the following values. The values can be configured in the order Lockout > Force Switch > Manual Switch > No Mode. For example, if Force Switch is currently configured on the device, then you can configure only Manual Switch or No Mode values. You cannot configure Lockout when Force Switch is configured.
  - **Lockout**: Prevents a working interface from switching to a protect interface. For example, if the protect interface is configured as circuit 1, the Lockout option prevents the protect interface from becoming active.
  - **Manual Switch:** Manually switches a circuit to a protect interface, unless a request of equal or higher priority is in effect.
  - **Force Switch**: Manually switches a circuit to a protect interface, unless a request of equal or higher priority is in effect. For example, if the protect interface is configured as a particular circuit, the force command sets the protect interface to active.
  - **No Mode**: Removes the current APS/MSP request configuration from the protection group on the device.

Note To clear the protection group of SONET or SDH , choose either SONET or SDH protection group ID and then click the delete (X icon).

Step 7 To view similar parameters associated with UPSR/SNCP interfaces, click the **UPSR/SNCP** tab.

You can view information such as the protection group number, working and protecting members configured on the device, the active paths for the group, and its current protection status. This information cannot be modified.

Note During shutdown or removal of IM that have UPSR/SNCP over SDH configured, you can validate the changes in the UI and check for the Online Insertion Removal (OIR) of each interface module. Use the **show protection-group** command.

- To view the following status changes:
  - Manual —The status is displayed whrn you maually configure the SNCP protection group.
  - Clear—Clears previously set external command.
  - Auto—The status is displayed when you configure the SNCP protection group for the first time.
  - Force—The status is displayed when you manual switch over.
  - Fail—The status is displayed when protected and working paths are down.
  - Signal Failure—The status goes to SF when there is a link failure.
  - Signal Degrade—The status is displayed when the working path is down.
  - Lockout—Prevents a working interface from switching to a protect interface.

Step 8 Choose **Circuit Emulation** > **SONET and SDH**.

Step 9 To view or configure the ACR Controller, High-order Path, Low-order Path parameters, click the relevant tabs. Click the SONET or SDH hyperlink that you want to modify, and then click the Edit icon at the top right corner of the page. For more information about configuration of SDH see, Configure Modes of SDH in EPNM, on page 337, Configure SDH Parameters , on page 336 and Configure SDH Line and Section Parameters, on page 338 SDH VC Configuration Parameters for SAToP, on page 340 SDH T1/E1 Configuration Parameters, on page 339 SDH T3/E3 Configuration Parameters, on page 339

Use the **ACR Controller** tab to view the virtual SONET Access Circuit Redundancy (ACR) /SDH Access Circuit Redundancy (ACR) details for SONET/SDH protection groups .

Configure Clocking for CEM

Clocking modes define multiple ways to achieve the same clock in the transmitting and receiving ends of a CEM circuit. Cisco EPN Manager enables you to configure clock recovery and distribution in these ways:

- Synchronous Clocking—with synchronous clocking, PDH (TDM) lines on the source and destination are synchronized to the same clock delivered by some means of physical clock distribution (SONET, SDH, and so on). The clock on the particular TDM line can be delivered from.
  - Line—the transmit clock is from the receiver of the same physical line.
  - Internal—the controller will clock its sent data using the internal clock.
  - Free Running—the transmit clock is taken from line card and can be derived from an internal free running oscillator.
  - Recovered—the transmit clock is derived from an in-band pseudowire-based active clock recovery on a CEM interface.

  To set these clocking values in Cisco EPN Manager, see Configure CEM Interfaces.
- Adaptive Clocking—adaptive clocking is used when the routers do not have a common clock source. The clock is derived based on packet arrival rates based on dejitter buffer fill level. You can set the size of the Dejitter Buffer (in the range of 1-32) during provisioning of CEM services in Cisco EPN Manager. The size of the Dejitter Buffer determines the ability of the circuit to tolerate network jitter.
- Differential clocking—differential clocking is used when the cell site and aggregation routers have a common clock source but the TDM lines are clocked by a different source. The TDM clocks are derived from differential information in the RTP header of the packet concerning the common clock. Differential clock recovery is based on time stamps received in the RTP header.

To configure clock recovery for CEM:

Step 1 Click the **Configuration** tab, then click the **Device Details** left side tab.

Step 2 Choose **Clock** > **Recovered Clock**.

Step 3 To add a new interface from which the clock source must be derived, click the Add (‘+’) icon.

Step 4 To edit the existing recovered clock configuration, click the Recovering Interface hyperlink and click the ‘Edit’ icon at the top right of the page.

Step 5 Specify the following recovered clock values:

a. Enter a unique numerical value for the **Recovered Clock ID** for easy identification of the recovered clock configuration. This ID can then be used to associate the CEM interfaces directly with this the recovered clock configuration.

b. From the **Recover Mode** drop-down list, choose:

- **Adaptive**—when devices do not have a common clock source, the recovered clock is derived from packet arrival rate on the controller selected as the Protecting Member for the associated Protection Group.
- **Differential**—when the edge devices have a common clock source, the recovered clock is derived from timing information in packets and the related difference from the common clock.

c. Enter a unique numerical value for easy identification of the **CEM Group Number**. This identifies the CEM group associated with the clock.

d. Choose the required controller from the **Recovering Interface** drop-down list. This controller associated with the clock is the virtual CEM interface from which the clock is derived when a backup clock source is required.

Step 6 Click **Save**.

Your changes are saved and deployed to the device.

CEM Interface (PDH, SONET, and SDH) Field Descriptions

To configure the CEM parameters listed in the following table:

Step 1 Configure the required CEM parameters on SONET, PDH, HOP, and HOP controllers. See, Configure Interfaces for CEM, on page 323.

Step 2 Configure clock distribution and recovery for CEM. See Configure Clocking for CEM, on page 330.

Table 21: CEM Interface (SONET, SDH, and PDH) Field Descriptions

Fields	Descriptions	Values	Descriptions	Applicable Controller Modes
Rate	Identifies the rate at which the data gets transported. It depends on the SFP (Small Form-factor Pluggable).	LR_DSR_OC1_STM0	Indicates the layer rate supported on the channelized OC-1 line with STM level 0. OC-1 is an optical carrier network line with transmission data rate of up to 51.84 Mbit/s.	STS1E
		LR_DSR_OC3_STM1	Indicates the layer rate supported on the channelized OC-3 line with STM level 1. OC-3 is an optical carrier network line with transmission data rate of up to 155.52 Mbit/s.	SONET /SDH
		LR_DSR_OC12_STM4	Indicates the layer rate supported on the channelized OC-12 line with STM level 4. OC-12 is an optical carrier network line with transmission data rate of up to 622.08 Mbit/s.	SONET/SDH
		LR_DSR_OC48_STM16	Indicates the layer rate supported on the channelized OC-48 line with STM level 16. OC-48 is an optical carrier network line with transmission data rate of up to 2.4Gbps.	SONET /SDH
		LR_DSR_OC192_STM64	Indicates the layer rate supported on the channelized OC-192 line with STM level 64. A channelized OC-192 line with STM level 64. OC-192 is an optical carrier network line with transmission data rate of up to 9.6Gbps.	SONET /SDH

Fields	Descriptions	Values	Descriptions	Applicable Controller Modes
Mode	Identifies the type of channelization, such as Synchronous Transport Signal of level n (STS-n), for high-order and low-order paths.	High- Order Path values: STS3C, STS12C, STS48C, STS192C, T3, UNFRAMED, VT15, VT2, and CT3. Low Order Path values: VT15, T1, and E1. **Note** Supported modes for STS1E: High- Order Path values: T3 and UNFRAMED Low Order Path values: CT3 and VT15	• STS-n: Mode with Synchronous Transport Signal (STS) channelization of level n. • T1, E1, T3, and E3: Indicates the channelization mode used on the controller. T1 or E1 circuit has a transmission data rate of up to 1.544 Mbit/s. The T3 or E3 circuit has a transmission data rate of up to 44.736 Mbit/s. • VT 1.5: Indicates that the controller is a virtual tributary network line with transmission data rate of up to 1.728 Mbit/s. • VT 2: Indicates that the controller is a virtual tributary network line with transmission data rate of up to 2.304 Mbit/s. • Unframed: Indicates that a single CEM channel is used for all T1/E1 timeslots.	HOP and LOP
		VC4_16C, VC4_4C, VC4, AU4_VC12, AU4-VC11, AU3-VC12, AU3-VC11, T3, E3, VC1X, TUG3	Supported SDH modes	HOP and LOP
Clock Source	Identifies the source of the clock signal sent on SONET or SDH ports.	Line	Controller clock its sent data using the clock recovered from the line's receive data stream.	All
		Internal	The transmit clock is taken from line card and can be derived either from an internal physical line.	All
		Recovered	In-band pseudowire-based activeclock recovery on a CEM interface which is used to drive the transmit clock.	SONET, SDH, HOP, and LOP.

Fields	Descriptions	Values	Descriptions	Applicable Controller Modes
Framing	Framing mode used for the CEM channel.	CRC and NO_CRC.	CRC: represents the faming type with cyclic redundancy check.	SONET/ SDH
		Unframed, DSX1_ESF, DSX1_SF, Auto Detect, C_BIT, and M13.	• Unframed: indicates that a single CEM channel is used for all timeslots. • DSX1_SF: indicates that the DS1 type of interface has the framing type as super frame. SF uses 12 frames per super frame for in-band signaling extraction. • DSX1_ESF: indicates that DS1 type of interface has the framing type as extended super frame. ESF uses 24 frames per ESF.	PDH, HOP, LOP, and STS1E.
Loopback	Specifies the loopback value associated with the CEM interface.	Local, Network Line, Remote, Remote Line, Network Payload, and Unknown.	For a detailed explanation about the different loopback values, refer the latest IOS Command References.	All
		Diag, Local Payload, Remote ESF Payload, Remote ESF Line, Remote ESF Line CSU, Remote ESF Line NIU, Remote Iboc, Remote Iboc CSU, Remote Iboc FAC1, Remote Iboc, and FAC2.	—	PDH
Protection Role	Identifies the priority based on which the recovered clock must be obtained.	WORKING	The recovered clock is obtained from a clock with the highest priority.	SONET/ SDH
		PROTECT	The recovered clock is obtained from a clock with a lower priority than the primary clock.	SONET/ SDH
Cable Length	Sets the transmission attenuation according to the length of the cable. For example, if you choose short 115, the cable length is from 0 to 115 feet. Choose Short 220 if the cable length is from 110 to 220 feet, and so on. Your values are between Short 110 to Short 550, Shot LT 225, and Long GT 225.			PDH
Line Coding	Line encoding method for the controller: • For E1, the options is Alternate Mark Inversion (AMI). • For T1, the options are AMI and bipolar with 8 zero substitution (B8ZS).			PDH

Fields	Descriptions	Values	Descriptions	Applicable Controller Modes
Channelization Mode	Indicates the channelization mode that must be used on the controller. A T1 or E1 circuit has a transmission data rate of up to 1.544 Mbit/s. Your values are T1, E1, and Unchannelized. **Note** For T3 controllers view or modify the channelized T1/E1 properties and for E3 controller view or modify the channelized T1/E1 properties.			PDH
Protection Group Number	Identifies the protection number or ACR group.			SONET /SDH
Protection Loopback Name	Identifies the name of the loopback interface on the device.			SONET/ SDH
Protection Loopback IP	Identifies the IP address of the loopback interface on the device.			SONET/ SDH
Protection Revertive Time Protection Non-Revertive Time	For any failure on working line, the software switches to protection line and when the working line recovers, it waits based on the revertive timer and reverts back to working line as active link. When the signal fails, the software switches to the protection line and does not automatically revert back to the working line. This is the default option.			SONET /SDH
Operational Status	Operational status of the CEM interface. This field cannot be edited.	Up, Down, and Not-Applicable.	• Down— the interface is down. • Not-Applicable— the interface has an unknown operational status. • Up— the interface is up.	SONET, SDH, HOP, LOP, and STS1E.
Admin Status	Administrative status of the CEM interface.	Up, Down, and Not-Applicable.	• Up— the CEM interface is administratively up. • Down— the CEM interface is administratively down. • Not-Applicable— the administrative status is unknown.	SONET, SDH, HOP, LOP, and STS1E.
Recovered Clock ID	Unique identifier for the clock settings associated with the CEM interface. To configure the Recovered Clock ID, see Configure Clocking for CEM.			PDH, HOP, and LOP.
Aug Type	An Administrative Unit Group (AUG) consists of one or more administrative units occupying units, defined positions at STM level. AUG-3 Grouping and AUG-4 Grouping are the supported Aug Types.			SDH

Configure SDH Parameters

To configure SDH CEM channelization modes refer the following table.

Table 22: Controller Modes and Supported Port Types

SDH Modes	CEM	Ports	Applicable Controller Modes
VC4_16c	CEP	STM16	HOP
VC4_4c	CEP	STM4, STM16	HOP
VC4	CEP	OC3/STM1, OC12/STM4, OC48/STM16	HOP
VC1X	CEP	OC3/STM1, OC12/STM4, OC48/STM16	HOP
TUG3-E3	SATop	OC3/STM1, OC12/STM4, OC48/STM16	HOP
TUG-3-T3	SATop	OC3/STM1, OC12/STM4, OC48/STM16	HOP
VC11_T1	SATop	OC3/STM1, OC12/STM4, OC48/STM16	LOP
VC12_E1	SATop	STM1, STM4, STM16	LOP
VC11	CEP	OC3/STM1, OC12/STM4, OC48/STM16	LOP
VC12	CEP	OC3/STM1, OC12/STM4, OC48/STM16	LOP

Configure Mediatype Controllers

Each SFP port (16-19) can be configured as STM1, STM4, STM16. You must select the MediaType controller to configure and enter the controller configuration mode. You must configure the controller as a SDH port.

```
To configure MediaType Controller:
enable
configure terminal controller
MediaType 0/0/16
mode sdh
end
```

Configure Rates on SDH Ports

```
To configure rate on SDH ports:
 enable
configure terminal
controller MediaType 0/0/16
mode sdh
end
```

Note The configuration of no form of the command is not supported. To restore to the default condition, use no mode sdh command under Mediatype controller after removing all configuration under that port.

Configure Modes of SDH in EPNM

A Synchronous Transport Module (STM) signal is the Synchronous Digital Hierarchy (SDH) equivalent of the SONET STS. In this document, STM term refers to both path widths and optical line rates. The paths within an STM signals are called administrative units (AUs). An AU is the information structure that provides adaptation between the higher-order path layer and the multiplex section layer. It consists of an information payload (the higher-order VC) and an AU pointer, which indicates the offset of the payload frame start relative to the multiplex section frame start. The AU-3 pointer is composed of 3 bytes; the AU-4 pointer is composed of 9 bytes. The payload of the STM-1 frame consists of one AU-4 unit or three AU-3 units. Augment Mapping An administrative unit group (AUG) consists of one or more administrative units occupying fixed, defined positions in an STM payload. Augment mapping is supported at STM1 level.

The following types of augment mapping are supported:.

- Augment Mapping AU-4

Note This is the default augment mapping mode

- Augment Mapping AU-3

The supported modes of SDH are:

- AU-4_16c (VC4-16c)
- AU-4_4c (VC4-4c)
- AU-4 (VC4)
- AU-4 — TUG-3 — DS3
- AU-4 — TUG-3 — T3
- AU-4 — TUG-3 — E3
- AU-4 — TUG-3 — TUG-2 — VC-11 — T1
- AU-4 — TUG-3 — TUG-2 — VC-12 — E1
- AU-4 — TUG-3 — TUG-2 — VC-11
- AU-4 — TUG-3 — TUG-2 — VC-12
- AU-3—T3

- AU-3 — TUG-2 — VC-11—T1
- AU-3 — TUG-2 — VC-12—E1
- AU-3 — TUG-2 — VC-11
- AU-3 — TUG-2 — VC-12
- AU-3 — E3

To configure Administration Units Group (AUG) mapping; for example, Configuring AU-3 or AU-4 Mapping use the following configuration commands:

```
configure terminal
 aug mapping [au-3 | au-4]
end
```

Note The **aug mapping** command is available only when the SDH framing is configured. The AUG mode is AUG-4 by default and it is supported at STM-1 level.

Configure SDH Line and Section Parameters

The following parameters affect SDH configuration at the line and section levels.

Loopback

Sets a loopback to test the SDH ports.

- local —Loops the signal from Tx to Rx path. Sends alarm indication signal (AIS) to network.
- network— Loops the signal from Rx to Tx path.

Configuring Line Loopback

```
 To configure loopback:
enable
configure terminal
controller sdh 0/0/16
loopback [local | network]
end
```

Note To restore the system to its default condition, use the no form of the command.

Clock Source

Specifies the clock source, where:

- line—The link uses the recovered clock from the line.
- internal— The link uses the internal clock source. This is the default setting.

```
To configure clock, use the following commands:
enable
configure terminal
controller sdh 0/0/16
```

```
clock source [line | internal]
end
```

Note The default mode is internal. To restore the system to its default condition, use the no form of the command.

Configuring Network-Clock SDH

```
To configure network-clock SDH, use the following commands:
enable
configure terminal
controller sdh 0/0/16
clock source line
end
enable
configure terminal
network-clock input-source 1 controller sdh 0/0/16
end
```

SDH T1/E1 Configuration Parameters

The following parameters affect SDH T1/E1 configuration:

- Clock — Specifies the clock source for T1 or E1 interface.
- Description — Specifies the description of the controller.
- Loopback — Sets the T1 or E1 interface in the loopback mode.

Configuring SDH T1/E1 Parameters

```
To configure T1/E1 parameters:
enable
configure terminal
controller sdh 0/0/16
rate stm4
au-3 1
mode vc1x
tug-2 1 payload vc11
t1 1 loopback [local | network line]
t1 1 clock source [line | internal | recovered]
end
```

SDH T3/E3 Configuration Parameters

The following parameters affect SDH T3/E3 configuration:

- Clock— Specifies the clock source for T3 or E3 link.
- Loopback— Sets the T3 or E3 link in the loopback mode.

Configuring SDH T3/E3 Parameters

```
To configure SDH T3/E3 parameters configuration:
enable
configure terminal
controller sdh 0/0/16
rate stm4
au-4 1
```

```
mode tug 3
tug-3 1
mode e3
e3 1 clock source [line | internal | recovered]
e3 framing [m13 | c-bit ] (applicable to for mode e3)
e3 1 loopback [local | network line]
e3 bert pattern 0s interval 2
tug-3 2
mode t3
t3 1 clock source [line | internal | recovered]
t3 framing [m13 | c-bit ] (applicable to for mode t3)
t3 1 loopback [local | network line]
end
```

Note This is applicable to AUG mapping AU-4 mode T3 and AU-3 mode T3.

SDH VC Configuration Parameters for SAToP

The following parameters affect SDH VC configuration:

- Clock — Specifies the clock source for VC.
- Loopback— Sets the VC in the loopback mode.

Configuring VC Parameters

```
To configure VC parameters:
enable
configure terminal
controller sdh 0/0/16
rate stm4
au-3 1
mode vc1x
tug-2 1 payload vc11
vc 1 loopback [local | network]
vc 1 clock source internal
end
```

Synchronize the Clock Using Sync-E, BITS, and PTP

Synchronous Ethernet (Sync-E):

Using Cisco EPN Manager, you can enable frequency synchronization to provide high-quality bit clocks synchronization over Ethernet interfaces. Synchronous Ethernet (Sync-E) provides this required synchronization at the physical level.

To do this you need to configure Sync-E that helps routers identify the clock in the network with the highest priority. This clock is also called the Primary Clock. All the other devices (members) on the network reset their clocks based on the primary clock's settings. Messages are constantly exchanged between the primary clock and its members to ensure efficient continued synchronization of all clocks in the network. Cisco EPN Manager enables you to specify this primary clock and also set the Sync-E parameters at the global and interface levels. Once the Sync-E properties have been configured, you can view the logical hierarchy and topology between the devices on the network topology overlay.

Note Sync-E configuration is supported only on Ethernet interfaces.

Building Integrated Timing Supply (BITS):

BITS is the method by which clocking information is provided by a Building Integrated Timing Supply (BITS) port clock. In Sync-E, Ethernet links are synchronized by timing their bit clocks from high-quality, stratum-1-traceable clock signals in the same manner as SONET/SDH. Operations messages like SSM and ESMC maintain Sync-E links and ensure that a node always derives its timing from the most reliable source.

Precision Time Protocol (PTP):

In networks that employ TDM, periodic synchronization of device clocks is required to ensure that the receiving device knows which channel is the right channel for accurate reassembly of the data stream. The Precision Time Protocol (PTP) standard:

- Specifies a clock synchronization protocol that enables this synchronization.
- Applies to distributed systems that consist of one or more nodes communicating over a network.

PTP uses the concept of primary and subordinate devices to achieve precise clock synchronization. With the help of Cisco EPN Manager, you can use PTP to configure the primary device which periodically starts a message exchange with the subordinate devices. After noting the times at which the messages are sent and received, each subordinate device calculates the difference between its system time and the system time of the primary device. The subordinate device then adjusts its clock so that it is synchronized with the primary device. When the primary device initiates the next message exchange, the subordinate device again calculates the difference and adjusts its clock. This repetitive synchronization ensures that device clocks are coordinated and that data stream reassembly is accurate. The PTP clock port commands are used to modify PTP on individual interfaces. Once the PTP properties have been configured, you can view the logical hierarchy and topology between the devices on the network topology overlay.

Note Due to the limitations on the device, you can configure a maximum of four clock sources on interface modules, with a maximum of 2 per interface module. This limitation applies to both Sync-E and TDM interfaces.

To configure Sync-E, BITS, and PTP:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device's name hyperlink.

Step 3 Set the global Sync-E properties.

a) Click the **Device Details** tab.
b) Click **Clock > Sync-E**. All available Sync-E global settings are listed.
c) To create a new set of global Sync-E properties, click the **'+'** icon. You can create only one set of Sync-E global parameters.
d) Specify the global parameters for Sync-E. For a detailed description about these parameters, see the table below.
e) Click **Save**.
Your changes are saved and the global Sync-E configuration is deployed to the device. You can now specify the interfaces that you want to associate with this configuration.

Step 4 Specify the associated interfaces and interface specific Sync-E parameters.

a) Select the Sync-E global configuration created in the above steps from **Clock > Sync-E**.
b) Click the **Interface Input Source** tab.
c) Click **'+'** to specify the required interfaces.

You can configure only one interface per synchronization type.

d) Use the **Interface Name** drop-down menu to select the required interface.
e) Specify the interface level Sync-E parameters. For a detailed description about these parameters, see table below.
f) Click **Save**.

Step 5 Specify the frequency settings for BITS (for XE devices):

a) Click the **Device Details** tab.
b) Click **Clock > BITS-Frequency**.
c) Specify the following BITS values:

- Source Slot: The values are RO and R1.
- Priority: Numeric value within the range 1–250.
- Clock Type: The values are 2.048 MHz and 10 MHz.

d) Click **Save**.

Step 6 Specify the interface settings for BITS:

a) Click the **Device Details** tab.
b) Click **Clock > BITS-Interface**.
c) Specify the following BITS values:

For XE devices:

- Source Slot: The options are RO and R1.
- Priority: Numeric value within the range 1–250.
- Clock Type: The options are E1 and T1.

Note The SSM option must be OPTION2_GEN1 or OPTION2_GEN2 to configure the BITS interface as T1.

For XR devices:

- Clock Interface: The options are BITS0_IN, BITS0_OUT, BITS1_IN, and BITS1_OUT.
- Clock Type: The options are E1, T1, J1, _2M, and _64K.

d) Click **Save**.
e) Specify the BITS clock settings for the interface:

1. Navigate to **Clock > BITS-Interface** and click on the Source Slot of the BITS Interface settings created in the above step.
2. Click the **Bits Clock Settings** tab and specify the clock settings as described in the table below.
3. Click **Save**.

Step 7 Specify the PTP clock settings:

a) Click the **Device Details** tab.

b) Click **Clock > PTP**.
c) Click '+' to specify a new set of PTP values, or click the Clock Mode hyperlink and then click the Edit icon at the top-right corner of the page.
d) Specify the following common PTP parameters and click **Save**.

- **Clock Mode**: Choose the mode of PTP operation. Your options are **Ordinary**, **Boundary**, and **E2E Transparent**. E2E stands for End-to-end transparent clock mode.
- **Domain No**: Enter the number of the domains used for PTP traffic. A single network can contain multiple domains. Range is 1–127 .
- **Hybrid Clock**: Enable or disable hybrid cloud.

e) Click the Clock Mode hyperlink and click the **Port** tab to specify the port details that must be associated with the common properties.
f) Specify the following Port details and click **Save**.

- **Port Name**: Enter the name of the PTP port clock.
- **Port Mode**: Choose the PTP role of the clock, Primary or Subordinate.
- **Loopback Interface Number**: Enter the clock identifier derived from the device interface.
- **Announce Timeout**: Enter the number of PTP announcement intervals before the session times out. Range is 1–10.
- **Delay Request Interval**: Choose the time when the interface is in PTP primary mode and the selected interval is specified to member devices for delay request messages. The intervals use base 2 values.
- **Sync Interval**: Choose the time interval for sending PTP synchronization messages.
- **Announce Interval**: Choose the time interval for sending PTP announcement packets.

g) Click the Port Name hyperlink and click the **Clock Source** tab.
h) Click '+' to add a new interface, or click the source address hyperlink and click Edit at the top-right corner of the page.
i) Specify the **Source Address** and the **Priority** for the clock.

- **No Priority**- Assigns the priority value as 0.
- **Priority 1**- Checks the first value for clock selection. The clock with the lowest priority takes precedence and the value 1 is assigned.
- **Priority 2**- If two or more clocks have the same value in the Priority 1 field, the value in this field is used for clock selection. This assigns the priority value of 2.

j) Click **Save** to deploy your changes to the device.

For detailed descriptions about all Sync-E global and interface level parameters, see the table below:

Fields	Descriptions
Clock > Sync-E Common Properties (Global Level)	
Automatic Selection process	Indicates the type of method used for synchronization of the clocks. The values are: Automatic, Forced, Manual, and Cisco. Note- You can configure only one interface per synchronization type.

Fields	Descriptions
Clock Type	Indicates the Ethernet Equipment Clock (EEC) option to be used: Option 1-represents EEC-Option I of the European time zone. Option 2-represents EEC-Option II of the American time zone.
QL Mode Enabled	Indicates whether the clock is to be used with the Quality Level (QL) function: Enabled or Disabled.
ESMC Enabled	Indicates the status of the Ethernet Synchronization Message Channel (ESMC): Enabled or Disabled.
SSM Option	Indicates the Synchronization Status Message (SSM) option being used: Option 1-represents ITU-T Option I Option 2- GEN1-represents ITU-T Option II Generation 1 Option 2- GEN2-represents ITU-T Option II Generation 2
Hold Off Time (global level)	Indicates the length of time (in milliseconds) for a device to wait before issuing a protection response to a failure event. A valid range is 300–1800 milliseconds.
Wait To Restore Time (global level)	Indicates the length of time (in seconds) to wait after a failure is fixed before the span returns to its original state. A valid range is 0–86400 seconds.
Revert Enabled	Specifies whether the network clock is to use Revertive mode: Enabled or Disabled.
Sync-E > Interface Input Source (Interface Level) Properties	
Interface Name	Name and hyperlink of the Gigabit or 10 Gigabit interface associated with Sync-E.
Active clock	Indicates whether the interface is currently chosen as the active clock. This interface can either be a primary or secondary interface, however, the interface that is currently enabled for Sync-E is considered to be the active interface.
Priority	Indicates the value used for selecting a Sync-E interface for clocking if more than one interface is configured. Values are 1–250, with 1 being the highest priority. The highest priority clock represents the primary clock.
Hold Off Time (interface level)	Indicates the length of time (in milliseconds) to wait after a clock source goes down before removing the source. A valid range is a value 300–1800 milliseconds.
Wait To Restore Time (interface level)	Indicates the length of time (in seconds) to wait after a failure is fixed before the interface returns to its original state. A valid range is a value 0–86400 seconds.

Fields	Descriptions
Rx Exact/QL Use	Indicates the QL Receive function with which the clock must be used.
Tx Exact/QL Send	Indicates the QL Transmit function with which the clock must be used.
Clock > BITS-Frequency and BITS-Interface Properties	
Source Slot	Indicates whether the clock source is R0 or R1 (for XE devices).
Clock Interface	Indicates whether the clock source is BITS0_IN, BITS0_OUT, BITS1_IN, or BITS1_OUT (for XR devices).
Priority	Indicates the value used for selecting a BITS interface for clocking if more than one interface is configured. Values are 1–250, with 1 being the highest priority. The highest priority clock represents the primary clock.
Clock Type	Indicates whether the clock type that must be used is from an E1 line or a T1 line (for XE devices). For XR devices, the line can be E1, T1, J1, 2M, or 64K. For BITS Interface parameters, the clock type indicates the frequency values that must be associated with the clock. Supported clock types for XE devices: • BITS Frequency: Supported options are 2.048_MHz and 10_MHz. • BITS Interface: Supported options are T1 and E1. Supported clock types for XR devices: • BITS Interface: Supported options are T1, E1, J1, 2M, and 64K.
Bits Framing	Framing values (such as CAS) that must be associated with the BITS configuration. • Supported Bits Framing values for XE devices: E1_CAS_CRC4, E1_CAS, E1_CRC4, E1_FAS, T1_D4, T1_ESF, and T1_SF • Supported Bits Framing values for XR devices: E1_CRC4, E1_FAS, J1_D4, J1_ESF, T1_D4, and T1_ESF
Impedance	The impedance value that is associated with the clock in OHMS format. Supported impedance values are 75 ohms and 120 ohms.
Bits Sub Framing	The supported Bits sub framing values for XR devices with E1 clock type are SA4, SA5, SA6, SA7, and SA8.

Fields	Descriptions
Line Code	The line code value that must be associated with the BITS interface. Supported line code values for XE devices: • For E1 interface: The values are AMI and HDB3. • For T1 interface: The values are AMI and B8ZS. Supported line code values for XR devices: • For E1 interface: The values are AMI and HDB3. • For J1 interface: The values are AMI and B8ZS. • For T1 interface: The values are AMI and B8ZS.
Line Build Out	The line build-out value that must be associated with the BITS interface. This field is supported only for T1 interface. Supported line build-out values for XE devices: • For T1 interface: The values are 0-133ft, 133-266ft, 266-399ft, 399-533ft, and 533-655ft. Supported line build-out values for XR devices: • For T1 BITS0_OUT interface: The values are 0, 1, 2, 3, and 4. • For T1 BITS1_OUT interface: The values are 0, 1, 2, 3, and 4.

What to do next

(Optional) You can view the Sync-E and PTP device properties on the network topology overlay. See Show Clock Synchronization Networks on a Network Topology Map, on page 197:

- **Sync-E overlay**: shows the topology and hierarchy of the Sync-E network. It shows the primary clock and the primary and secondary clock inputs for each device.
- **PTP overlay**: shows the clock synchronization tree topology, the hierarchy of the Precision Time Protocol, and the clock role of each device in the tree (primary, boundary, subordinate, or transparent).

Configure IP SLAs (TWAMP Responder/TWAMP Light Responder)

The IETF Two-Way Active Measurement Protocol (TWAMP) defines a standard for measuring round-trip IP performance between any two devices that support TWAMP. The TWAMP-Control protocol is used to set up performance measurement sessions by sending and receiving performance-measurement probes. Once a session is created, TWAMP test packets are transmitted to help calculate the performance statistics including

packet loss, delay etc. TWAMP Light differs from standard TWAMP by simplyifing the control protocol used to establish the test sessions.

TWAMP Responder is supported for both Cisco IOS XE (NCS 42xx) and Cisco IOS XR (ASR 9000, NCS 540, NCS 560, NCS 5500) devices. The TWAMP Light Responder is supported only for Cisco IOS XR (ASR 9000, NCS 540, NCS 560, NCS 5500) devices. TWAMP Light supports IPv4 and IPv6 addresses while standard TWAMP is supported for IPv4 addresses only.

For more information on configuring TWAMP interfaces, see:

- Configure TWAMP Responder, on page 347
- Configure TWAMP Light Responder, on page 347

Configure TWAMP Responder

When you configure TWAMP using Cisco EPN Manager, the device you select is configured as a TWAMP server. The TWAMP server listens for connection and control requests on the specified port. The Inactivity Value that you specify will be configured as the inactivity timer (in seconds) for a TWAMP control session.

Use the following procedure to add or edit entries for TWAMP:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

Step 3 Click **Device Details** tab.

Step 4 Choose **IP SLA > TWAMP Responder** to add or edit the TWAMP Responder configuration.

Step 5 Click the '+' icon to add the TWAMP parameters to the selected device. To edit existing parameters, click the Port Name hyperlink and click the Edit icon at the top right corner of the page. You can only add one set of TWAMP parameters per device.

Step 6 Edit the following parameters as necessary. All parameters are mandatory.

- **Port**- Use a numeric value between 1 and 65535 to specify the port that must be configured for the TWAMP server to listen for connection and control requests. The default value is 862.
- **Inactivity Timeout**- Use a numeric value between 1 and 604800 to specify the time that must be configured as the inactivity time (in seconds) for a TWAMP responder test session. The default value is 900 seconds.
- **Server Inactivity Timeout**- Use a numeric value between 1 and 6000 to specify the time that must be configured as the TWAMP server inactivity time (in seconds) for a TWAMP control session. The default value is 900 seconds.

Step 7 Click **Save** to deploy your changes to the device.

Configure TWAMP Light Responder

Use the following procedures to manage interfaces for the TWAMP Light Responder:

- Add a TWAMP Light Responder, on page 348
- Edit TWAMP Light Responder configuration, on page 348

• Delete a TWAMP Light Responder configuration, on page 349
• Commands to view TWAMP Light session details, on page 349

Add a TWAMP Light Responder

Use the following procedure to add an entry for TWAMP Light Responder:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

Step 3 Click **Device Details** from the tab on the left.

Step 4 Choose **IP SLA** > **TWAMP Light Responder**.

Step 5 Click the '+' icon in the **TWAMP Light Responder** page.

Step 6 Enter appropriate values in the displayed fields. Hover your mouse over the tooltip next to a particular field to get information on the range of permissible values.

a) **Session ID** - Specify a Session ID. You can configure up to 65535 test sessions.
b) **Timeout** - (optional) Specify the inactivity time between 60 and 86400 (in seconds) for a TWAMP Light responder test session. Default is No Timeout.
c) **Local IP address** - Specify an IPv4 address or IPv6 address.
d) **Local Port** - Use a numeric value between 1 and 65535 to specify the port you want to configure for the session.
e) **Remote IP address** - Specify an IPv4 address or IPv6 address.

Note If the specified **Local IP address** is an IPv4 address, then the **Remote IP address** must be an IPv4 address. Similarly, if the specified **Local IP address** is an IPv6 address, then the **Remote IP address** must also be an IPv6 address.

f) **Remote Port** - Use a numeric value between 1 and 65535 to specify the port for the session.
g) **VRF Name** - Select any VRF Name from the drop-down list.

Step 7 Click **Save** to deploy your changes to the device.

Edit TWAMP Light Responder configuration

To edit an existing TWAMP Light Responder configuration:

Step 1 Choose **Configuration** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

Step 3 Click **Device Details** tab.

Step 4 Choose **IP SLA** > **TWAMP Light Responder**.

Step 5 Click **Session ID** to edit parameters of the selected session. Click the Edit icon to change the parameters.

Note Only **Timeout** can be modified.

Step 6 Click **Save** to deploy your changes to the device.

Delete a TWAMP Light Responder configuration

To delete an existing TWAMP Light Responder configuration:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.
Step 2 Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.
Step 3 Click **Device Details** from the tab on the left.
Step 4 Choose **IP SLA** > **TWAMP Light Responder**.
Step 5 Select the check box next to the **Session ID** you want to delete.
Step 6 Click '**X**' and then click **Delete** to confirm and delete the selected configuration.

Commands to view TWAMP Light session details

Use the following commands to view session details on the device.

Command	Usage
`show ipsla twamp session`	To list all TWAMP Light sessions that are enabled.
`show running-config ipsla responder twamp-light test-session <test session ID>`	To view details of a specific TWAMP Light session.

Configure Interfaces

Using Cisco EPN Manager, you can configure your CE and Optical Interfaces using the following configuration options:

Before you configure the interfaces, ensure that the device's Inventory Collection status is 'Completed'.

- Configure Ethernet Interfaces and Subinterfaces, on page 350
- Configure Loopback Interfaces, on page 351
- Enable or Disable Tunnel Interfaces, on page 353
- Configure Switch Port Interfaces, on page 353
- Configure Ethernet Interfaces, on page 353
- View Virtual Template Interfaces, on page 354
- View VLAN Interfaces, on page 354
- Configure Network Team (Link Aggregation), on page 774
- Create or Modify an IP Access-List to Filter Network Traffic , on page 775
- Configure Protection Profiles, on page 368
    - Change the Loopback Settings on an Optical Interface, on page 355
    - Continuous Verification of the Connection Status, on page 356

Configure Ethernet Interfaces and Subinterfaces

The Configuration tab on the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can create, edit, delete, enable, and disable these interfaces.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Interfaces > Ethernet**.

Step 5 To add an Ethernet subinterface:

a) Choose an Ethernet interface and click **Add Subinterface**.

Note This button is enabled depending on the device that you select. For example, on Cisco ASR903 devices, this button is disabled.

a) In the Basic Configuration area, at a minimum, enter the **Interface Number** (if not already populated) and optionally provide a description for the subinterface.
b) In the **VLAN Number** field, enter a numerical value that can be used to represent the VLAN ID for this subinterface. Note that only the 802.1Q type of encapsulation is supported.
c) To use the same VLAN number as the native VLAN ID, enable the **Native VLAN** checkbox.
d) In the **Dataplane Loopback** drop-down menu, select the value that must be set as the loopback value. Your options are: **Blank** (makes no change in the configuration), **None** (removes the Ethernet loopback from the interface), **Internal**, and **External**. The value that is already configured on the device is highlighted in the bold font.
e) If you are creating an IPv4 subinterface, in the IPv4 Interface area, select an **IP Type**. Your options are:

  • None

- Static IP, with the IP address and subnet mask.
- DHCP IP, with the pool name.
- DHCP Negotiated, with the hostname and client ID (None, Interface, Port Channel).

You can also enter a secondary IP address with mask.

f) If you are adding an IPv6 subinterface, in the IPv6 Address area, select a type from the **Add** drop-down list. Your options are: Global, Unnumbered, Link Local, Auto Configuration, and DHCP.

- Global, with the IP address and subnet mask, and type (General, EUI-64, Anycast, CGA).
- Unnumbered, and enter text in the Interface Unnumbered To text box.
- Link Local, auto-configured or manually-configured (requires IPv6 address).
- Autoconfiguration.
- DHCP (with option to enable two-message exchange for address allocation).

If you choose to edit an existing interface or subinterface, you are allowed to change all values except the Interface Number value.

Note To avoid unusual behavior, do not use the § character in the Description field.

g) Click **Save** to add the subinterface to the selected interface of the device.

Step 6 To enable, disable, or delete interfaces and subinterfaces, select the interfaces and click the appropriate buttons.

The Delete Subinterface button may only be enabled on some supported devices, such as, Cisco ASR903 devices.

Step 7 Click **Save** to deploy your changes to the device.

Configure Loopback Interfaces

You can change the loopback state of an interface to test how your optical network is performing. Before changing the loopback setting, ensure that the device is either in Managed state or ideally in Complete state.

To change the loopback settings on an interface:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Interfaces > Loopback**.

Step 5 To specify a new loopback interface, click **Add**.

a) In the Basic Configuration tab, specify the **Loopback Interface Number** (if not pre-populated).

b) If you are creating an IPv4 loopback interface, specify an **IP Type**:

- None.
- Static: along with the IP address and subnet mask of the static IP address.
- DHCP IP: along with the DHCP pool name.

You can also enter a secondary IP address with its mask so that it can be used as the backup loopback interface.

c) If you are adding an IPv6 loopback interface, in the IPv6 Address area, select a type from the Add drop-down list. Your options are:

- Global- which also requires you to specify the IP address, subnet mask, and type (General, EUI-64, Anycast, CGA).
- Unnumbered- which requires you to enter text in the Interface Unnumbered To text box.
- Link Local- which is either auto-configured or manually-configured and only applies to requires IPv6 address.
- Autoconfiguration
- DHCP- which also allows you to set the option to enable two-message exchange for automatic address allocation.

Step 6 To edit an existing loopback interface, select the interface and click the **Edit** button to change only the speed, duplex, and other settings. The Interface Number cannot be edited.

Step 7 To enable the above loopback settings on the interfaces, select the required loopback process and click **Enable**.

Step 8 Click **Save** to deploy these configuration changes on the device.

Enable or Disable IOT Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can enable and disable IOT interfaces. This is applicable for EM, C3794, X.21, and serial interfaces (RS232, RS485, and RS422). If you Enable/Disable an interface all the Controllers will be listed for the above technologies.

Note If an interface is not present, commands for Enabling/Disabling of interface will not be sent to the device.

Note There is no QoS support for all the IOT services.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 In the **Chassis View** tab, view all serial controllers that are listed for the configured CEM or channel group.

Step 4 In the **Device Details** tab, view, enable, or disable all the serial interfaces and also the X.21 interfaces.

Step 5 Choose **Interfaces > Serial**.

Step 6 In the right pane, view all the list of serial controllers that are supported in EPNM and check one controller at a time to enable or disable.

Step 7 Click **Save**.

Enable or Disable Tunnel Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can enable and disable these interfaces.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab and choose **Interfaces > Tunnel** from the left side menu.

Step 4 To enable or disable a tunnel interface, select the interfaces and click the Enable or Disable button.

Note MPLS TE tunnel interfaces can be enabled or disabled here. For information on creating or editing MPLS TE tunnels, see Create and Provision an MPLS TE Tunnel, on page 589.

Configure Switch Port Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can edit, delete, enable, and disable these interfaces.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Note The **Configuration** tab appears only for the supported devices.

Step 4 Choose **Interfaces > Switch Port**.

Step 5 To edit an interface, select the interface and click **Edit**.

- Choose and Administrative Mode: Static, Trunk 802.1Q, or Routed.
- Enable or disable the port fast setting, and adjust the speed and duplex, if needed.

Step 6 Click **Save**.

Configure Ethernet Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can edit, delete, enable, and disable the ethernet interfaces.

Limitations:

- For NCS 4202 and ASR 901, speed and duplex are supported for mediatype RJ45 Gigabit Ethernet.

- Dropdowns are disabled for speed and duplex if mediatype is not configured.
- For other IOS/XE device types, drop downs are disabled and you will not be able to set speed and duplex values from EPNM.
- For NCS 4202, if speed is set as 1 Gig, only full duplex option is supported, else for 10 and 100 Mbps, both half and full duplex is supported.
- For ASR 901, for all 10, 100, 1000 Mbps speed, half and full duplex is supported.
- If you select Auto option in speed dropdown, both speed and duplex dropdown will reflect Auto and user will be able to set the negotiation mode as Auto in this case.
- Select speed and duplex manually from dropdown and "no negotiation auto" command will be sent to device with appropriate speed and duplex values.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Note The **Configuration** tab appears only for the supported devices.

Step 4 Choose **Interfaces > Ethernet**.

Step 5 To edit an interface, select the interface and click **Edit**.

You can now modify the required details.

Step 6 Click **Save**.

View Virtual Template Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Note that you can only view the virtual template interfaces from this page. You cannot add, edit, enable, or disable the interfaces.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Interfaces** > **Virtual Template**.

View VLAN Interfaces

The Configuration tab in the Device Details page lists the current interface configurations on the device. Note that you can only view the VLAN interfaces from this page. You cannot add, edit, enable, or disable the interfaces.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Interfaces** > **Vlan**.

Configure Optical Interfaces

Using EPN Manager, you can configure your optical interfaces to change their admin settings, enable standard FEC modes on them, modify their payload settings, and change their loopback settings. To do this, use the Configuration tab in the Device Details page which lists the current interface configurations on the device. Depending on your device configuration and user account privileges, you can create, edit, delete, enable, and disable these interfaces.

You can configure optical interfaces in the following ways:

Change the Loopback Settings on an Optical Interface

You can change the loopback state of an interface to test how your optical network is performing. Before changing the loopback setting, ensure that the device is either in Managed state or ideally in Complete state. The interface that you want to modify must be in Maintenance (OOS, MT) admin state. EPN Manager allows you to edit the loopback settings only on SONET, SDH, Ethernet, FC/FICON, and OTN interface types.

To change the loopback settings on an interface:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Configuration** tab.

Step 4 Choose **Optical Interfaces** > **Maintenance** > **Loopback**.

The interfaces of the selected device are displayed along with their loopback settings. Interfaces that are not supported, for example, Data Storage, OTS, or Video, are not displayed.

Step 5 To edit the loopback settings, select the interface name (hyperlink) and click **Edit** to make your changes. Ensure that the device is in Managed or Complete state and the interface is in Maintenance (OOS, MT) admin state.

a) Internal—this applies the same configuration applied in Terminal loopback.
b) Line—this applies the same configuration applied in Facility loopback.
c) No_Loopback—Select this option to set no loopback values on the interface.

Before you change the loopback state ensure that you first clear the current loopback setting using the No_loopback option from the drop-down menu and then re-apply the setting of your choice.

Step 6 Click **Save** to save your edits.

A pop-up notification notifies you about the status of your changes.

Note If the Edit task fails, check if the device is in Managed or Completed state and ensure that Cisco EPN Manager is in sync with the device configuration. If not, resync the device with Cisco EPN Manager. See, Collect a Device's Inventory Now (Sync), on page 449.

Continuous Verification of the Connection Status

Using the Connection Verification feature, you can view the power levels of optical interfaces and verify the interfaces for connectivity and insertion loss. Verifying the connectivity indicates whether the cable is in a connected state and verifying that the insertion loss indicates whether the cable loss is within an expected value. The parameters for insertion losses are collected for every possible optical path inside the network element in order to predict possible failures.

Using Cisco EPN Manager you can view the Connection Verification parameters and opt to enable or disable Connection Verification on interfaces. You can also set the acknowledgment values for associated alarms.

To verify the connection status for your optical interfaces:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Configuration** tab.

For Cisco NCS 2000 series and Cisco ONS series devices, this choice is under the Device Details tab that is at the top of the Device Details page.

Step 4 To enable or disable the Connection Verification feature and set the common threshold vales, click **Optical Interfaces > Provisioning > Connection Verification**.

Step 5 Click the Edit icon at the top-right corner of the page to edit common parameters.

Step 6 Enter the following threshold parameters for the selected device and click **Save**:

- Connection Verification Enabled- Set to True or False to enable or disable this feature on the selected device.
- Fail IL Threshold (dB)- Enter a numerical value ranging 0–20. When this threshold value is exceeded, an alarm is generated.
- Degree IL Threshold (dB)- Enter a value lesser than the failed IL threshold value.

Step 7 Click **Optical Interfaces > Maintenance > Connection Verification Entry**.

For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Device Details tab that is at the top of the Device Details page.

Step 8 Click the A Side hyperlink to view the following values of the connection:

- A Side- Displays the originating slot for connection verification.
- Z Side- Displays the destination slot for connection verification.
- Last Refresh- Displays the date and time when the connection verification and insertion loss verification was run previously.
- Connectivity Last Change- Displays the date and time when the connectivity information was previously changed.
- Connectivity Verification- Displays the status of connectivity:
  - Connected- Cable or patch cord is connected.
  - Disconnected- Cable or patch cord is disconnected.
  - Disabled- Cable or patch cord is excluded from connection verification.
  - Not Measurable- Power source not detected; cable or patch cord cannot be tested for connection verification.
  - Not Verified- Cable or patch cord is yet to be tested for connection verification.
- Excess Insertion Loss (dB)- Display the excess insertion loss that is higher than the set threshold.
- Insertion Loss Last Change- Displays the date and time when the insertion loss verification information was previously changed.
- Display names for- A and Z Side, A and Z Side Modules- identification names of the connection for A and Z Side, and A and Z Side Modules.
- Insertion Loss Verification- Displays the insertion loss verification status which is one of the following:
  - Not Verified- Cable or patchcord is yet to be tested for insertion loss verification (this is the default status at first boot).
  - Not Measurable- Power source not detected; cable or patchcord cannot be tested for insertion loss verification.
  - Loss OK- Cable or patchcord insertion loss is within expected value.
  - Degrade- Cable or patchcord insertion loss is degrading.

    When the Insertion Loss is greater than the Insertion Loss Degrade Threshold and less than the Insertion Loss Fail Threshold, the Insertion Loss Verification of the patch cord is Degrade. The corresponding row of the patch cord in the Connection Verification pane is highlighted in yellow.
  - Fail- Cable or patchcord insertion loss crossed the fail threshold. When this condition occurs, the patchcord is highlighted in the GUI to indicate the Fail condition.

When the Insertion Loss is greater than the Insertion Loss Fail Threshold, the Insertion Loss Verification of the patch cord is Fail. The corresponding row of the patch cord in the Connection Verification pane is highlighted in orange.

- Disabled- Cable or patchcord is excluded from connection verification.

- Acknowledgement- Displays the set value for the associated alarms. The values can be set to True or False.

Step 9 In the **Connection Verification Action** drop-down menu, choose an action that must be taken when the configured threshold values are reached, and click **Save**. Your options are: **Verify loss and connectivity**, **Disable verification**, and **Acknowledge loss alarm**.

Step 10 (Optional) Select one of the following values to specify how alarms must be generated with respect to the Connection Verification parameters:

- **Acknowledge Loss Alarm** - allows the interfaces to operate beyond the Fail IL Threshold thresholds without raising an alarm. If the Fil IL Threshold further increases, alarms are raised again.
- **Clear Acknowledge** - indicates that the Fail IL Threshold thresholds are set to default and alarms are re-evaluated. If thresholds are exceeded, an alarm is raised.

Configure PRBS on ODU Controllers

Pseudo Random Binary Sequence (PRBS) is a testing mechanism used to ensure that the selected overhead bytes can be used to transport the header and trailer data safely. Both the transmitting node and receiving node must be aware that PRBS testing is taking place. To do this you can use Cisco EPN Manager to enable appropriate PRBS modes on the nodes. Cisco EPN Manager allows you to configure PRBS only on the nonchannelized ODU controllers of an optical device.

PRBS also enables trunk ports to generate the PRBS_31 pattern and detect PRBS_11, PRBS_23, and PRBS_31 patterns.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Navigate to the **Device Details** tab.

Step 4 Choose **Optical Interfaces > Maintenance > PRBS Configuration**. All ODU controllers and their current PRBS parameters are displayed. If the controllers are not listed, ensure that the above stated prerequisites are met.

Note For Cisco NCS 1004 series devices, this option is available under **Chassis View** > **Configuration** > **Controllers** > **PRBS Configuration**.

Step 5 To configure PRBS, click the controller's name hyperlink and click the Edit icon at the top-right corner of the page.

Step 6 Make your modifications to the following parameters.

a) In the **Admin State** drop-down list, select a valid admin state for the ODU controller. Your options are **00S-MT** (maintenance), **OOS-DSBLD** (disabled), and **IS** (in-service).

The PRBS parameters can be edited only if you set the Admin State to 00S-MT (maintenance) state.

To edit only the admin state of the controller, set the PRBS mode to Disabled, and choose the admin state of your choice.

b) Select the PRBS Test value as **Enabled** or **Disabled**.

c) Select the PRBS mode for the controller. When you set one controller with the values in column 1 (see below), ensure that the second controller (node 2) is set with the corresponding values shown in the second column of this table:

Controller 1 Mode (Node 1)	Controller 2 Mode (Node 2)
Source	Sink
Sink	Source
Source-Sink	Loopback
Loopback	Source-Sink

d) From the **Pattern** drop-down list, select one of the following PRBS patterns. This pattern is either generated or detected by the line cards:

- NONE
- PN11
- PN23
- PN31
- INVERTEDPN11
- INVERTEDPN31

Step 7 Click **Save** to deploy the updated configuration to the device.

Step 8 (Optional) To verify, view updated PRBS parameters in the **Configuration** tab for the selected controller, under **Optical Interfaces > Provisioning > PRBS**. To run a PRBS test on ODU UNI circuits, see, Run PRBS Test on Circuits (ODU UNI), on page 672.

Enable and Disable OSC

Using Cisco EPN Manager, you enable or disable the Optical Service Channel (OSC) terminations on the interfaces of optical devices. OSC can be configured on OC3 lines, and on FastEthernet (FSTE) and GigabitEthernet (GigE) interfaces of the following cards:

- Transmission Network Control System (TNCS)
- Transport Node Controller - Enhanced (TNCE)
- Transport Node Controller (TNC)

For ONS15454 NEs, the supported interfaces are OC3 interfaces of the following cards:

- Optical Service Channel Modem (OSCM)
- Optical Service Channel and Combiner/Separator Module (OSC-CSM)

To configure OSC on optical devices:

Step 1 Choose **Configuration > Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Configuration** tab.

For Cisco NCS 2000 series and Cisco ONS series devices, this choice is under the Device Details tab that is at the top of the Device Details page.

Step 4 Choose **Optical Interfaces >Provisioning > Comm Channels**.

All configurable G709 enabled interfaces of the selected device are displayed.

Step 5 Click the **OSC** tab.

Step 6 Choose the communication channel that that you want to configure by clicking the communication channel's name hyperlink.

The communication channel name and current OSC setting is displayed.

Step 7 Click the Edit icon at the top right of the page.

Step 8 Use the **OSC** checkbox to enable or disable OSC on the selected communication channel.

Step 9 Click **Save**.

Your changes are saved and the updated configuration is deployed to the device. To verify, view the OSC settings for the selected communication channel under **Optical Interfaces > Provisioning > Comm Channels**.

View and Acknowledge Unverified Alarms

Based on the alarm generated on your devices, you can view the details of the alarm in Unverified status and then mark them Acknowledged so that they no longer appear as unread alarm notifications on the device. To do this:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its **Device Details** page.

Step 3 Click the **Configuration** tab.

Step 4 Choose **Optical Interfaces** > **Maintenance** > **Unverified Alarms** to view the alarms with the Unverified status.

Step 5 Once you have reviewed the alarms and taken the required action, select the alarms, and click the **Acknowledge** button to mark these alarms Verified directly on the device.

Provision Optical Interfaces

You can use Cisco EPN Manager to enable the following configuration options on your optical devices.

Note The following configuration options are enabled or disabled depending on the device that you select. To check whether your device supports these options, see Supported Devices for Cisco EPN Manager.

- **Ethernet MTU**

Using Cisco EPN Manager you can configure the MTU values on the Ethernet interfaces of your optical devices. The MTU is the Maximum Transmission Size, in bytes, of a packet passing through the interface. You can use Cisco EPN Manager to modify the MTU values on all Ethernet interfaces except Gigabit Ethernet and Fast Ethernet interfaces on TNC and ECU modules.

To verify that your new Ethernet MTU values are configured on the device, navigate to your device's Device Details page and click the Ethernet Interface tab.

- **GMPLS**

  Using Generalized Multi-Protocol Label Switching (GMPLS), you can define and view the fiber and alien wavelength parameters that are used during GMPLS circuit creation. It ranges the packet-based data on the MPLS protocol to allow the creation and maintenance of channels across the networks. It supports non-packet switching devices. This means that GMPLS extends the packet-based MPLS protocol to allow creation and maintenance of tunnels across networks that consist of non-packet switching devices. GMPLS tunnels can traverse Time-Division Multiplex (TDM) interfaces and switching types.

  To configure GMPLS, you can use the Configuration tab in Cisco EPN Manager which allows you to configure GMPLS on all LMP enabled optical controllers. The enabling of LMP which is a prerequisite for GMPLS configuration can also be done using the same Configuration tab.

Note You cannot disable GMPLs on LMP enabled controllers that are part of active optical circuits.

- **Packet Termination**

  Using Cisco EPN Manager you can set up packet termination on the ODU controllers of your optical devices. To do this, ensure that packet termination is preconfigured on the device for Ethernet packets. You can then edit the configuration that is already created on the device and discovered by Cisco EPN Manager.

  To configure packet termination, you must specify the Termination Mode and Mapping Mode values.

- **LMP**

  The Link Management Protocol (LMP) helps in managing channels and links that are required between nodes for routing, signaling, and link management. LMP is also used to manage the Traffic Engineering (TE) link. It allows multiple data links into a single Traffic Engineering (TE) link that runs between a pair of nodes.

  To create an LMP neighbor using Cisco EPN Manager, you need to specify the neighbor's name, link ID, router ID, and interface ID, and the common link and interface IDs. You can add only one LMP link per controller on your optical device.

  While the LMP configuration can be successfully deployed to a single device using Cisco EPN Manager, for LMP to function effectively, you need to configure it on both sets of devices that are participating in the link. This ensures that the LMP link is activated.

  Limitations:

  - You cannot edit the Numbering value of an LMP link after it has been created. To edit the Numbering value, delete the LMP link and recreate it with the new Numbering value.
  - You cannot have duplicate Neighbor Router IDs between two LMP neighbors.

- When you add an LMP link, ensure that the controller is not already associated with another LMP link. This causes your deploy to fail.

- **OTN Topology**

  You can use the Configuration tab to add or modify the topology instance and Area ID associated with an optical OTN controller. If the controller does not have a preconfigured Topology Instance and Area ID, Cisco EPN Manager automatically sets the topology instance to OTN and the Area ID to 0.

  Cisco EPN Manager does not allow you to use the same topology instance and Area ID that is already preconfigured on other controllers. To know the Topology Instance and Area ID that is preconfigured on the device, go to **Maps > Topology Maps > Network Topology**.

- **NNI**

  You can configure your optical interfaces to act as network-node interfaces (NNIs). An NNI indicates that the interface connects to other network nodes. Cisco EPN Manager allows you to configure NNIs on the OTU controllers of your optical device. These interfaces can further be configured to act as source and destination ports.

  If a device is not part of a topology, configuring its NNI controller creates an OTN topology instance for that controller with an Area ID 0.

  You can create only one NNI configuration per controller for every controller present on the device.

  Note: You cannot delete NNI controllers that are preconfigured with a Topology Instance.

- **Breakout**

  Enabling breakout on your optical devices utilizes the multilane architecture of the optics and cables to enable you to split single higher density ports into multiple lower density ports. For example, a 100G port can be configured to operate as 10 different 10G ports. Or a single 40G port can act as four different 10G ports. To configure breakout using Cisco EPN Manager, see the table below.

  Prerequisite:

  Ensure that Breakout is preconfigured on the interface by changing the interface's Port Mode value to Breakout. See Change the Port Mode/Payload and Breakout Settings, on page 371. This changes all other port mode parameters of that interface to 'None' enabling breakout on the port, thus allowing you to configure lanes. You can add up to 10 lanes per interface.

  Limitations:

  - All lanes that belong to a particular interface must have the same mapping type.
  - OTU2 and OTU2e controllers are supported only if they are in the packet termination mode.
  - In Cisco NCS 5.2.4x devices, breakout lanes can only be created when the port modes are of type Ethernet.
  - 10G clients that are mapped to OPU2e framing type are not supported.
  - Breakout cannot be configured on SONET and SDH controllers.

  Example configuration:

  If you select a controller optics 0/0/0/0 and enable Breakout with GFPF as its mapping mode and with a framing value of OPU2, then the configuration pushed to the device is:

```
controller optics 0/0/0/0 breakout-mode 1 ethernet framing opu2 mapping gFpF
```

- **Performance Monitoring**

  Performance Monitoring (PM) helps you gather performance counters for system maintenance and troubleshooting. You can retrieve current and historical PM counters at regular intervals. You can enable and disable performance monitoring on OTU and ODU controllers of an optical device.

  To configure performance monitoring at the TCM controller level, you must configure OTN interfaces and their associated TCM performance counters, see:

  - Reference—Performance Counters for OTN-FEC Interfaces, on page 961
  - Reference—Performance Counters for OTN-ODU Interfaces, on page 961
  - Reference—Performance Counters for OTN-OTU Interfaces, on page 962

- **Channelize ODU (LO) Controllers:**

  Associate your ODU controllers with multiple lower-order ODU subcontrollers and configure tributary port number (TPN) and tributary slots (TS) for those ODU subcontrollers. A valid range of TPN is 1–80. If a TS string is separated using a colon (:), this indicates individual tributary slot. If a TS string is separated using an en-dash (-), this indicates a range of tributary slots.

  When you select the ODU level for the subcontrollers, ensure that the subcontroller's ODU level is lower than that of the main controller you are associating it with. For example, if you are associating subcontrollers with an ODU controller of ODU3 level, then the subcontrollers can be of levels ODU2, ODU1, or ODU0.

- **Configuring OTDR Settings:**

  Using this feature, you can configure OTDR scans to begin automatically on a fiber span that has been repaired or on the startup of an OSC channel. To do this, ensure that the 'Auto Scan on LOS' parameter is enabled. A fiber is considered to be repaired when the LOS on the fiber is cleared and an alarm is raised based on the following criteria:

  - If you check the Enable Absolute Threshold checkbox, the 'OTDR-LOSS-THR-EXCEEDED' alarm is raised when the insertion loss measured for the OTDR scan is greater than the Absolute Event Loss Threshold (dB) value configured.
  - If the total back reflection for the OTDR scan is less than the Total Back Reflection (dB) value that you specify.
  - If the Absolute Pass Fail Criteria is disabled, the Loss and Back Reflection values from the baseline scan in the previous release are considered as threshold values. In this scenario, the OTDR-LOSS-THR-EXCEEDED alarm is raised.

  Depending on how you want the auto scans to be triggered, you can configure the following parameters:

  - Auto Scan on Span Loss Increase- OTDR scan starts automatically on the fiber if the measured span loss on the fiber is greater than the threshold value configured. The default threshold value is 2.
  - Enable OLR continuous measurement on Rx direction-measures the span loss in the LINE-RX port (input) of the card depending on the configured threshold value.
  - Enable WDM Side from WSON Provisioning-prevents creation of circuits when the Loss and Back reflection threshold values are crossed during an OTDR scan.

You can configure the Event Loss Threshold value within which the total span loss on the fiber is permitted. If the measured span loss on the fiber is greater than the Event Loss Threshold value, then the OTDR scan is triggered on the fiber.

- **Configure Automatic Laser Shutdown (ALS):**

  Automatic Laser Shutdown (ALS) is a technique used to automatically shutdown the output power of the transmitter if there are issues such as a fiber break. This is a safety feature that prevents dangerous levers of laser light from leaking out of a broken fiber, provided ALS is provisioned on both ends of the fiber pair. Once an interface has been shut down, you can configure the action that must be taken to restart the interface by setting the ALS mode to:

  - **Disabled mode**—If mode is disabled, ALS is disabled. Loss Of Signal (LOS) will not cause laser shutdown.
  - **Manual restart mode**—The laser is turned off when the ALS agent detects an LOS for 500 ms. After ALS is engaged, a manual command is issued that turns on the laser for the time period of the pulse width. The laser is turned on when the LOS has been cleared for 100 ms.
  - **Automatic restart mode**—The laser is shut down for the time period of pulse spacing when the ALS agent detects a LOS for 500 ms. Then, the laser automatically turns on for the time period of the selected pulse width. If an LOS still exists, then the laser is shut down again. This pattern continues until the LOS is cleared for 100 ms; then, the laser stays on.

  Cisco EPN Manager enables you to set the ALS mode, the ALS recovery interval (in seconds), and the recovery pulse width (in seconds). If the ALS Mode for the interface has been set to Manual Restart, you need to manually restart the interface. To do this, navigate to the device's Device Details page, choose **Optical Interfaces > Provisioning > Automatic Laser Shutdown**, locate the interface set to the Manual Restart ALS mode, and click the **Restart** button.

- **Using the SNTP Server to Set the Date and Time:**

  Simple Network Time Protocol (SNTP) is an internet protocol used to synchronize the clocks of computers to a time reference. Using the SNTP server ensures that all NEs use the same date and time reference. The server synchronizes the node’s time after power outages or software upgrades.

  To use the SNTP server to set the date and time, you must first specify the current time along with the time zone value, and then set the primary and backup servers that can be used as a point of reference for the date and time. Before you set the timezone values, ensure that the SNTP server values are not configured. When you delete an SNTP server, ensure that you first delete the Backup server and only then the Primary server. You cannot delete only the Primary server.

- **Configuring the Wavelength:**

  Cisco EPN Manager enables you to provision the wavelength frequency for your optics controllers. You can view the current wavelengths configured on the optics controllers and then depending on the type of card selected, you can change the wavelength frequency.

  You can configure the wavelengths on an optics controller only when it is configured as a DWDM optics port. The optics port must not be in the **In Service** state when you are changing the wavelength.

Table-Provisioning Optical Interfaces

To configure your optical devices with the above features:

Step 1 Choose **Configuration** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Configuration** tab.

Step 4 Navigate to the required configuration menu as described in the table below, and specify the required values.

Table 23: Table-Configuring Optical Interfaces

Task	Supported Interfaces/Controllers	Navigation	Notes
Configuring Ethernet MTU	All Ethernet interfaces except Gigabit/Fast Ethernet interfaces on TNC and ECU modules.	Optical Interfaces > Provisioning > Ethernet MTU	-
Configuring GMPLS	LMP enabled optical controllers.	Optical Interfaces > Provisioning > GMPLS	-
Configuring Packet Termination	ODU controllers preconfigured with Packet Termination.	Optical Interfaces > Provisioning > OTN > Packet Termination	Applicable only to Ethernet packets.
Configuring an LMP Neighbor	All optical controllers.	Optical Interfaces > Provisioning > LMP	Neighbor Router ID cannot be duplicated between neighbors
Configuring OTN Topology	All optical OTN controllers.	Optical Interfaces > Provisioning > OTN > Topology	-
Configuring NNI	All OTU controllers.	Optical Interfaces > Provisioning > OTN > NNI	-
Configuring Breakout	All optical controllers with Port Mode values set to ‘Breakout’.	Optical Interfaces > Provisioning > Port Mode > Breakout tab	-
Configuring Performance Monitoring	All OTU and ODU controllers.	Optical Interfaces > Provisioning > Performance Monitoring	-
Channelize ODU (LO) Controllers	All ODU controllers.	Optical Interfaces > Provisioning > ODU Channelization > Sub-Controllers tab	-
Configuring OTDR Settings	-	Optical Interfaces > Provisioning > OTDR Settings	-
Configuring ALS	All ALS supported interfaces	Optical Interfaces > Provisioning > Automatic Laser Shutdown	-

Setting the Date and Time using SNTP	-	• To specify the primary and backup servers for SNTP: Choose Optical Interfaces > Provisioning > NTP Settings. For Cisco NCS 2000 series devices, this option is under Chassis View > Configuration > General. • To specify the current time and time zone that can be used by SNTP: Choose Optical Interfaces > Provisioning > Time Zone Settings.	-
Configure Wavelength	All optics controllers	Optical Interfaces > Provisioning > Wavelength	-
Configure TCM and TTI	-	See Configure TCM and TTI Parameters, on page 369	-
Configure Protection Profiles	-	See Configure Protection Profiles, on page 368	-
Configure the Payload and Breakout Settings	-	See Change the Port Mode/Payload and Breakout Settings, on page 371	-
Configure the Admin Status	-	See Change the Admin Status of an Optical Interface, on page 367	-
Configure FEC Mode	-	See Configure OTN Interfaces, on page 372	-
Enabling and Disabling GCC	-	See, Enable and Disable GCC Connections, on page 373	-
Configure Squelch Mode	-	See, Configure Squelch Mode, on page 373	-

Change the Admin Status of an Optical Interface

Cisco EPN Manager enables you to change the admin state of an interface to enhance the performance testing abilities for your optical network. The Admin Status of an interface defines whether the interface is being managed by Cisco EPN Manager, whether it is down, or whether it is in maintenance mode. When the admin status of an interface is down, it indicates that the interface is in an unreachable state, or that the device is not supported by Cisco EPN Manager. Changing the admin status to Up enables Cisco EPN Manager to manage the interface and thus provide better monitoring capabilities. To change the admin state on an interface:

Step 1 Choose **Configuration** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Configuration** tab.

For Cisco NCS 2000 and Cisco ONS devices, this choice is under the Device Details tab that is at the top of the Device Details page.

Step 4 Choose **Optical Interfaces** > **Provisioning** > **Admin Status**.

The interfaces of the selected device are displayed along with their Admin State settings. Interfaces on which you cannot modify the admin state, for example, PCHAN and PLINE interfaces are not displayed.

Step 5 Click either the **Optical Controllers** or **Ethernet Controllers** tab to edit the required controllers.

Step 6 To edit the admin status, select the interface by clicking the interface's Name hyperlink, and then click the **Edit** icon at the top right corner of the page. Ensure that the device's inventory collection status is in Managed or Completed state.

Choose one of the following values:

a) **DOWN**—implies that the interface will be administratively down.
b) **UP**—implies that the interface will be administratively up.
c) **TESTING**— implies that the interface is in Maintenance state and that the administrator is performing tests using it.

Step 7 Click **Save** to save to deploy your changes to the device.

A pop-up notification notifies you about the status of your changes. To see an example of the admin status being changed on a Cisco NCS2K device, see Example: Change the Admin Status for Cisco NCS 2006 Interface, on page 375.

Note If the Edit task fails, check if the device is in Managed or Completed state and ensure that Cisco EPN Manager is in sync with the device configuration. If not, re-sync the device with Cisco EPN Manager as described in Collect a Device's Inventory Now (Sync), on page 449.

Change the Admin Status of an Optical Interface

Cisco EPN Manager enables you to change the admin state of an interface to enhance the performance testing abilities for your optical network. The Admin Status of an interface defines whether the interface is being managed by Cisco EPN Manager, whether it is down, or whether it is in maintenance mode. When the admin status of an interface is down, it indicates that the interface is in an unreachable state, or that the device is not supported by Cisco EPN Manager. Changing the admin status to Up enables Cisco EPN Manager to manage the interface and thus provide better monitoring capabilities. To change the admin state on an interface:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 For Cisco NCS 1000 series devices,

a) Open the **Chassis View** window, click the **Configuration** tab, and then **Controllers**.
b) To edit the admin status, select the interface (under the respective tabs like Optics, Ethernet, and so on).
c) Click the icon, which opens the **Edit** window.
d) Change the Admin Status and click **Save**.

Step 4 For Cisco NCS 2000 series and Cisco NCS 4000 series devices,

a) Navigate to **Device Details** > **Optical Interfaces** > **Provisioning**, and click **Admin Status**.
b) To edit the admin status, click the required interface hyperlink from the **Optical Controllers** or **Optical Controllers** tab.
c) Click the icon, which opens the **Edit** window.
d) Change the Admin Status and click **Save**.

Note Choose one of the following values while selecting the Admin Status:

- **DOWN**—implies that the interface is administratively down.
- **UP**—implies that the interface is administratively up.
- **TESTING**—implies that the interface is in Maintenance state and that the administrator is performing tests using it.

Configure Protection Profiles

Using Cisco EPN Manager, you can provision different protection profiles (or groups) for your optical devices. This ensures availability and improved reliability for these devices. Protection profiles define whether Automatic Protection Switching (APS) must be enabled on the cards and they also set the direction for traffic flow in case of failures. The cards on the device can either be set to support unidirectional regeneration of configuration or can be set to ensure that both transmit and receive channels will switch when a failure occurs on one.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.
Step 2 Click the device hyperlink to launch its Device Details page.
Step 3 Click the **Device Details** tab that is at the top of the Device Details page.
Step 4 Choose **Optical Interfaces** > **Provisioning** > **Protection Profile**.
Step 5 To add a protection profile, click the **+** symbol.
Step 6 Provide a unique name for the protection profile. The name is a mandatory field and should not contain space or exceed 32 characters.
Step 7 Select the required type for the protection profile. Your options are:

- **One plus one BDIR APS**- Enables one plus one Automatic Protection Switching (APS) and configures the card to be bidirectional.
- **One plus one UNIDIR APS**- Enables one plus one APS and configures the card to be unidirectional.
- **One plus one UNIDIR NO APS**- Enables one plus one with no APS and configures the card to be unidirectional.
- **One plus one PLUS R BIDIR APS** - Enables one plus one plus R APS and configures the card to be bidirectional.

Note
- BDIR (bidirectional) indicates that both transmit and the receive channels will switch if a failure occurs on one.
- UNIDIR (unidirectional) indicates that the card supports unidirectional regeneration of configuration. Hence the ports can only be used as the link source if they are transmit ports and as the link destination if they are receive ports.

Step 8 Select the protection mode for the profile as **Revertive** or **Non-Revertive**. Revertive mode ensures that the node returns traffic towards the working port post a failure condition after the amount of time specified as the Wait to Restore Time (step 9).

Step 9 Select the sub network connection mode as **SNC_N** (default), **SNC_I**, or **SNC_S**.

Step 10 When you select the sub network connection mode as **SNC_S**, you can then select TCM-ID value from the TCM drop-down list. By default, TCM-4 is selected once you select SNC_S as Sub Network Connection mode. You can change the TCM-ID column value from TCM4 to TCM1-TCM6 for SNC_S.

Note For SNC_I and SNC_N, you are not allowed to change the TCM-ID value. It should be set to **None**.

Step 11 Enter a value for the Wait to Restore Time in seconds using a number between 0 and 720. For any value greater than 0, ensure that the value is greater than 300 and in intervals of 30 seconds. The wait to restore time defines the time the system must wait to restore a circuit. If you have selected the protection mode as Revertive, then the default wait to restore time is 300, else it is 0.

Step 12 Enter a value for the **Hold Off Time** in milliseconds. This value defines the time the system waits before switching to the alternate path. The valid range is from 100 to 10,000 seconds. Default value is 0.

Step 13 Click **Save** to deploy the updated changes to your device.

Step 14 (Optional) To verify, view the updated protection profile parameters in the **Configuration** tab for the selected controller, under **Optical Interfaces > Provisioning > Protection Profile**.

Note The above-mentioned steps are not applicable for NCS2K devices.

Configure TCM and TTI Parameters

Using Cisco EPN Manager you can configure Tandem Connection Monitoring (TCM) and Trail Trace Identifiers (TTI) on ODU controllers of ODU Tunnel circuits. This helps you enable and disable performance monitoring capabilities on these controllers.

You can further monitor your device capabilities by configuring the threshold for signal failure and signal degradation in the TCM connections of these ODU controllers. You can also modify the source and destination access point identifiers. To do this, ensure that the following prerequisites are met.

Before you begin

- Ensure that the device's inventory collection status is 'Completed'.
- Ensure that the controllers are configured for Loopback. If not, change the controllers loopback settings under **Optical Interfaces** > **Maintenance** > **Loopback**. See Configure Loopback Interfaces, on page 351.

Note For the endpoints of an ODU UNI circuit, TCM is supported only on OTUx-ODUx controllers.

Step 1 Choose **Configuration** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Step 4 To configure TCM/TTI parameters, choose **Optical Interfaces** > **Provisioning** > **TCM Configuration**.

Alternatively you can navigate to the device's Chassis View tab, select a card from the Chassis Explorer, click the **Configuration** tab, and choose **OTN** > **Trail Trace Identifier**.

Note To configure TCM parameters for Cisco NCS 2000 series devices, navigate to the device's Chassis View tab, select a card from the Chassis Explorer, click the **Configuration** tab, and choose **OTN** > **Trail Trace Identifier**.

Step 5 To view or edit the TCM parameters of any of the listed controllers, click the TCM ID hyperlink of that controller.

Step 6 To edit these parameters, click the Edit icon at the top-right corner of the page.

Step 7 Make your changes to the following TCM parameters:

Editable TCM Parameters	Descriptions
State	Configures the state of TCM properties on the device as enabled or disabled.
Signal Failure Threshold	Configures the threshold value for signal failures on ODUk controllers. The values are E6, E7, E8, and E9.
Sent SAPI	Configures the source access point identifier of the TTI. Enter a value of up to 14 bytes in length.
Sent DAPI	Configures the destination access point identifier of the TTI. Enter a value of up to 14 bytes in length.
Sent Operator Specific String Type	Configures the type of the operator-specific string of the TTI as hexadecimal or ASCII type.
Sent Operator Specific String	Configures the operator-specific string of the TTI. Enter a value of up to 32 characters in length.
Performance Monitor	Enables or disables performance monitoring on an ODUk controller.
Signal Degrade Threshold	Configures the signal degrade threshold value. The values are: E6, E7, E8, and E9.
Expected SAPI	Configures the current source access point identifier of the TTI. Enter a value of up to 14 bytes in length.
Expected DAPI	Configures the current destination access point identifier of the TTI. Enter a value of up to 14 bytes in length.
Expected Operator Specific String Type	Configures the type of the operator-specific string of the TTI as hexadecimal or ASCII type.

Editable TCM Parameters	Descriptions
Expected Operator Specific String	Configures the operator-specific string of the TTI. Enter a value of up to 32 characters in length.

Step 8 Click **Save** to deploy the updated configuration to the device.

Step 9 (Optional) To verify, view the selected device's TCM parameters in the **Configuration** tab, under **Optical Interfaces** > **Provisioning** > **TCM Configuration.**

Step 10 (Optional) You can view these updated TCM and TTI parameters in the Device Details and Port 360 view of the selected device. See View Device Details, on page 83 and View a Specific Device's Interfaces: Device 360 View, on page 102.

Step 11 (Optional) The TCM parameters are also represented on the network topology overlay. To view these parameters, navigate to **Maps** > **Network Topology** and select an optical circuit with these associated TCM parameters.

Change the Port Mode/Payload and Breakout Settings

Using the Device Configuration tab, you can view and modify the type of the payload for packets on SONET and SDH interfaces and enable breakout on them. Before changing the payload setting, ensure that the device is in sync with Cisco EPN Manager. Enabling breakout on your optical devices utilizes the multilane architecture of the optics and cables to enable you to split single higher density ports into multiple higher density ports. For example, a 100G port can be configured to operate as ten different 10G ports. Or a single 40G port can act as four different 10G ports.

To change the payload and breakout setting on an interface:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab that is at the top of the Device Details page.

Step 4 Choose **Optical Interfaces** > **Provisioning**.

Step 5 Depending on the type of device that you have selected, choose **Payload** or **Port Mode**.

Step 6 Click the name (hyperlink) of the interface that you want to modify.

Common properties of the interface such as its name and its payload type are displayed.

Step 7 Click the name (hyperlink) of the OTN interface that you want to modify and click the Edit icon.

Step 8 Make your changes to the Port Mode, Framing, Mapping Type, Rate, and Bit Rate values. Ensure that these values do not exceed the card's bandwidth limitations.

Step 9 To associate breakout lanes for Ethernet and OTN packets on this interface, click the **Breakout** tab. This tab is only displayed if the device has breakout pre-configured.

a) Click the '+' icon to add a new lane. You can add up to 10 lanes per controller. To modify existing lanes, click the Lane hyperlink.

b) Specify the breakout parameters such as the lane number, the port mode and mapping type for the breakout lane, the owning port number, and the framing value.

Step 10 Click **Save** to deploy your changes to the device.

A pop-up notification notifies you about the status of your changes.

Note If the Edit task fails, check if the interface is in Managed state and ensure that Cisco EPN Manager is in sync with the device's configuration. If not, resync the device with Cisco EPN Manager. See Save Your Device Changes, on page 449. You also need to ensure that the payload does not exceed the card's bandwidth limitation.

Note Instructions given in Steps 6–10 are not applicable for NCS2K devices.

Configure OTN Interfaces

The FEC Mode defines an OTN circuit's forward error correction (FEC) mechanism. The forward error correction (FEC) mechanism provides performance gains for improved margins and extended optical reach. To change the FEC Mode setting to Standard, you need to use the Device Configuration tab.

Before changing the FEC mode setting, ensure that the admin state of the interface you are trying to modify is in Down (out of service) state with G709 configuration enabled. To enable G709 configuration, use the OTN Lines configuration in the Chassis view.

To change the FEC mode on an interface:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Configuration** tab.

For Cisco NCS 2000 series and Cisco ONS series devices, this choice is under the Device Details tab that is at the top of the Device Details page.

Step 4 Choose **Optical Interfaces** > **Provisioning**.

Step 5 Change the admin state of OTN interfaces for which FEC needs to be modified to Down. See Change the Admin Status of an Optical Interface, on page 367.

Step 6 Depending on your device type, choose one of the following and select the interface you want to modify:

- **OTN Lines** > **OTNFEC**
- **OTN** > **FEC**

All configurable G709 enabled interfaces of the selected device are displayed.

Alternatively, you can navigate to the device's Chassis View tab, select a card from the Chassis Explorer, click the **Configuration** tab, and choose **OTN** > **OTN Lines**. This option enables you to configure additional parameters such as enabling the sync messages, choosing the admin SSM, enable the Provide Sync parameter, and set the G709 value to true or false.

Step 7 Select the interface you want to edit, and click the Edit icon at the top right of the window.

Step 8 Select the required FEC Mode. The default is None.

Step 9 (Cisco NCS 2000 devices only) Select the required **SD BER** value. Signal Degrade Bit Error Rate (SDBER) condition indicates that a signal degrade alarm will occur for line degradation based on the threshold value that you set.

Step 10 Click **Save** to save your changes.

A pop-up notification notifies you about the status of your changes.

Note If the Edit task fails, check if the interface is in Managed or Completed state and ensure that Cisco EPN Manager is in sync with the device's configuration. You also need to ensure that G709 configuration is enabled on the device. To change the admin state of the interface see, Change the Admin Status of an Optical Interface, on page 367.

Enable and Disable GCC Connections

Cisco EPN Manager supports the provisioning of Generic Communication Channel (GCC) connection on the interfaces of optical devices. GCC can be configured on trunk ports of TXP or MXP cards and on OTN, OTU, and ODU controllers. The GCC configuration can be modified irrespective of the FEC modes and admin statuses configured on the interfaces.

To configure GCC on optical devices:

Step 1 Choose **Configuration** > **Network** > **Network Devices**. All Cisco EPN Manager devices are displayed.

Step 2 Select the optical device that you want to configure by clicking the device name hyperlink.

Step 3 Click the **Configuration** tab and choose **Optical Interfaces** > **Provisioning**.

Step 4 Depending on your device type, choose one of the following:

- **Comm Channels > GCC**
- **OTN > GCC**

All configurable G709 enabled interfaces of the selected device are displayed.

Step 5 Click the **OTU Controllers** or **ODU Controllers** tab based on the type of controller that you want to edit.

Step 6 To edit the GCC configuration of any of the listed controllers, click the controller's name hyperlink.

Step 7 Click the Edit icon at the top right of the page.

Step 8 Use the **GCC** check box to enable or disable GCC on the selected controller. The value configured on ODU controllers is GCC1 and that on OTU controllers is GCC0.

Step 9 Click **Save**. Your changes are saved and the updated configuration is deployed to the device.

To verify, view the GCC parameters for the selected controller under **Optical Interfaces > Provisioning.**

When GCC is enabled on a Cisco NCS device with 400G-XC trunk ports, Cisco EPN Manager discovers the OUT link between the trunk ports.

Configure Squelch Mode

Using Cisco EPN Manager, you can configure different squelch modes on the interfaces of optical devices. Squelch modes help shut down the far-end laser in response to certain defects. Squelch modes can be configured on OCH, OTN, SONET or SDH, FC or FICON, Ethernet, Video, and Data Storage interfaces of optical devices.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Configuration** tab.

For Cisco NCS 2000 series and Cisco ONS series devices, this choice is under the **Device Details** tab that is at the top of the Device Details page.

Step 4 Choose **Optical Interfaces** > **Provisioning** > **Squelch Mode**.

Step 5 Choose the interface that that you want to configure by clicking the interface's name hyperlink.

The interface's name and current squelch mode setting are displayed.

Step 6 Click the Edit icon at the top right corner of the page.

Step 7 Select the required squelch mode for the interface. Your options are:

- **DISABLE**- Squelch is disabled.
- **AIS-** Alarm Indication Signal (AIS) is enabled.
- **NONE**- Transparent mode is enabled.
- **SQUELCH**- Squelch is enabled.
- **ODU_AIS**
- **G_AIS**- Generis AIS is enabled.
- **NOS**- Squelch is disabled in FC payloads.
- **LF**

Step 8 Click **Save**.

Your changes are saved and the updated configuration is deployed to the device. To verify, view the squelch mode parameters of the selected interface under **Optical Interfaces** > **Provisioning** > **Squelch Mode**.

Configure Squelch Mode and Hold Off Timer for NCS 1004 interfaces

Squelch modes help shut down the far-end laser in response to certain defects. To configure squelch mode and hold off time for NCS 1004 interfaces:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page and then, select **Interfaces > Ethernet**.

Step 3 Select the interface that you want to edit and click the Edit icon.

The **Edit interface** window appears.

Step 4 Select a **Squelch Mode** from the drop down list.

Step 5 Enter the **Hold Off Timer**.

The hold off time ranges from 0 to 3000 milliseconds.

Step 6 Click **Apply**.

Example: Change the Admin Status for Cisco NCS 2006 Interface

This example illustrates how to change the admin status for a Cisco NCS 2006 VLINE interface. In this example, the configuration change is launched from the Device Details page, but under the **Device Details** tab. (For other devices, configuration changes are performed under the **Configuration** tab.)

Step 1 On the Device Details page under the **Device Details** tab, click the hyperlink for the interface you want to edit.

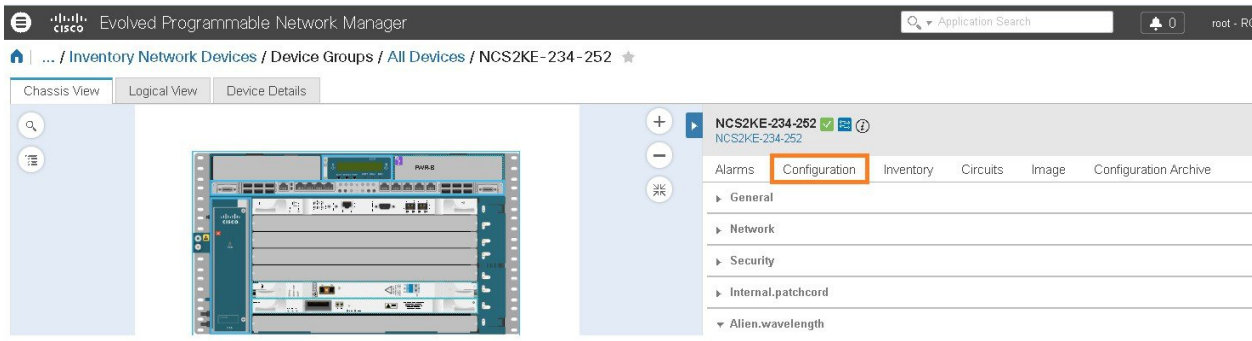
Step 2 In the interface's Common Properties window, click the Edit icon at the top right corner of the window.

Step 3 Choose a new setting from the **Admin Status** drop-down list, then click **Save**.

Configure Devices Using the Chassis View

You can configure devices and cards from the devices' Chassis View. This can only be done from the **Configuration** sub-tab in the Chassis View. The sub-tabs are displayed depending on the type of device you select in the **Network Devices** page.

Note This feature is available only for Cisco NCS 2000 and Cisco ONS devices.



Step 1 From the left sidebar, choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device's name hyperlink. The Chassis View tab for the device appears.

Step 3 In the right pane, click the **Configuration** sub-tab.

Step 4 Expand the **General** area, and then enter the details of the device such as the node name, node alias, and select the location where you want to provision the device.

Step 5 Set up the synchronization time for the device to synchronize with its associated controllers. You can either use the NTP/SNTP server time or set up a manual date and time for synchronization.

Step 6 Check the **Enable Manual Cooling** check box to manually change the cooling profile of the device. The cooling profile allows you to control the speed of the fans in the device's shelf.

Step 7 Click **Apply**. The changes in the settings are updated.

Step 8 Expand the **Network** area, select the network setting you want to modify, and then click the edit icon at the top left of the **Network** area. The **Edit Network General Settings** window appears.

Step 9 Modify the required settings, and then click **Apply**.

Note You cannot modify the Node Address, Net/SubnetMask Length, Mask, and MAC Address of the device.

Step 10 Configure security settings for a device. See Create and Manage Users and User Logins for a Device, on page 376.

Step 11 Configure the origination (TX) and termination (RX) patchcords for a device. See Configure Patchcords for a Device, on page 377.

Step 12 Configure the alien wavelength for a device. See Configure GMPLS and WSON Properties, on page 388.

Create and Manage Users and User Logins for a Device

Use this procedure to create users and assign roles to manage a device. You can also view the list of users who are accessing the device at a time.

Step 1 From the left sidebar, choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device's name hyperlink. The Chassis View tab for the device appears.

Step 3 In the right pane, click the **Configuration** sub-tab, and then expand the **Security** area.

Step 4 In the **Users** tab, click the + icon to add a user.

Step 5 Enter the user name.

Step 6 From the **Security Level** drop-down list, choose one of the following options:

- Retriever—Users with this security level can view and retrieve information from the device, but cannot modify the configuration.
- Maintenance—Users with this security level can retrieve information from the device and perform limited maintenance operations such as card resets, Manual/Force/Lockout on cross-connects or in protection groups, and BLSR maintenance.
- Provisioning—Users with this security level can perform all maintenance operations and provisioning actions except those that are restricted to super users.
- Super User—Users with this security level can perform all provisioning user actions, plus creating and deleting user security profiles, setting basic system parameters such as time, date, node name, and IP address, and doing database backup and restoration.

Step 7 Enter your password, and then click **Save**. The user is added to the Users table.

You can select a user to edit or delete the user. However, you cannot edit the user name. Moreover, you cannot delete a user who has added the device to Cisco EPN Manager.

In the Security area, click the **ActiveLogins** tab to view the list of users who have logged in to the device using CTC, TL1 session, or Cisco EPN Manager. You can choose to logout a user or multiple users when the maximum login sessions for a device is reached.

Configure Patchcords for a Device

The client card trunk ports and the DWDM filter ports can be located in different nodes or in the same single-shelf or multi-shelf node. A virtual link is required between the client card trunk ports and the DWDM filter ports. The internal patchcords provide virtual links between the two sides of a DWDM shelf, either in single-shelf or multishelf node. The patchcords are bidirectional, however, each direction is managed as a separate patchcord.

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

This procedure explains how to configure internal patchcords using the Chassis View using ANS (automatic node setup) for WDMs (wavelength division multiplexing). You can use the Chassis View to create and delete these internal patchcords. To configure origination (TX) and termination (RX) patchcords for a device:

Step 1 In the left sidebar, choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device's name hyperlink. The Chassis View tab for the device appears.

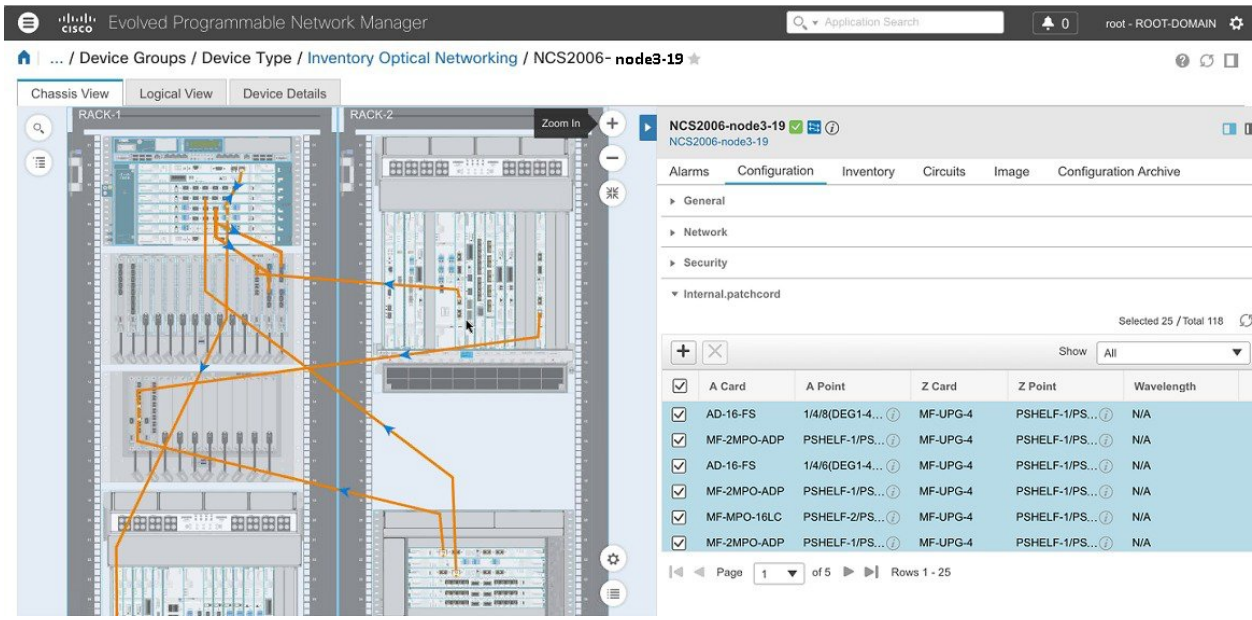
Step 3 In the right pane, click the **Configuration** subtab, and then expand the **Internal.patchcord** area.

Step 4 Click the + icon, and then choose the required origination (TX) and termination (RX) patchcords for the device.

Step 5 Click **Finish**. The patchcords are added to the Internal Patchcords table.

Note Once you have created the patchcord, you cannot modify it. However, you can delete it.

You can select a patchcord or multiple patchcords in the Internal Patchcords table to view the direction of the patchcords in the Chassis View of the device, which is displayed in the left pane (as shown in the figure below).



External Patchcords

External patch cords are required when the transponders or ITU-T line cards are installed in a device that does not house the OCH filter ports. You can configure the external patch cords using only the NCS 2000 Cisco Transport Controller. These patch cords then appear in the EPN Manager as OTS links.

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

The following procedure explains how to view external patchcords using the Chassis View:

Step 1 In the left sidebar, choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device name's hyperlink. The Chassis View tab for the device appears.

Step 3 In the right pane, click the **Configuration** subtab, and then expand the **Maintenance** area.

Step 4 Click the **External Patchcords** subtab.

Configure a Protection Group for a Shelf in a Device

Use this procedure to create a protection group for a shelf in a device.

Note You cannot configure a protection group for a rack.

Before you begin

Following are the prerequisites before creating a protection group for a shelf:

- To create a Y Cable protection group, ensure that two cards of the same type that are configured with client ports are plugged in to the same shelf.
- To create a Splitter protection group, ensure that at least one OTU2XP card that is configured with trunk port 3-1 and trunk 4-1, is plugged in to the shelf.

Step 1 From the left sidebar, choose **Configuration** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device's name hyperlink. The Chassis View tab for the device appears.

Step 3 Expand the Chassis View Explorer, and then select the shelf for which you want to configure the protection group.

Step 4 In the right pane, click the **Configuration** sub-tab, and then expand the **Protection** area.

Step 5 Click the + icon to open the Create Protection Group window.

Step 6 From the Type drop-down list, choose one of the following protection type:

- Splitter—This protection type is applicable only when a MXPP/TXPP card is used. These cards provides splitter (line-level) protection (trunk protection typically on TXPP or MXPP transponder cards).
- Y Cable—This protection type is applicable only when two transponder or two muxponder cards that are configured with client ports, are plugged in to the same shelf in a device.

Step 7 Choose a protect port and a working port for the shelf.

Note You will be able to select these ports only if you have completed the prerequisites listed at the beginning of this procedure.

Step 8 Choose if the protection type is unidirectional or bidirectional. In the bidirectional mode, a failure on a active interface triggers a switchover of the traffic from the active interface to the protecting/backup interface.

Step 9 Click the **Revertive** toggle radio button to revert the shelf from the protected port to the original port after the failure is fixed.

Step 10 Choose the hold off time in milliseconds. Hold off time is the period that the shelf on the protected port must wait before switching to the original port after the failure is fixed. The shelf can revert to the original port after the hold time expires. The minimum value of hold off time must be 0.5.

Step 11 Click **Apply**. The protection group is added to the Protection table.

Configure a Line Card for Cisco NCS 1004 Devices

A Cisco NCS 1004 device has two redundant field-replaceable AC and DC power supply units, and three redundant field-replaceable fans. It also provides a field-replaceable controller card. The device has SSD disks on the chassis and the controller card for resiliency. Each Cisco NCS 1004 chassis provides four line card slots and can host a line card.

To configure a line card on a Cisco NCS 1004 device:

Step 1 Launch the **Chassis View** as described in Open the Chassis View, on page 92.

Step 2 From the **Chassis Explorer**, select the card that you want to configure.

Step 3 Click the **Configuration** tab from the window displayed on the right and expand the **Card Configuration** drop-down.

Step 4 From the **Card Mode** drop-down list, select the applicable option.

The available options are **Slice Mode**, **Muxponder Mode**, and **Regen Mode** (some line cards do not have all three options).

Step 5 To add a new card configuration, click the **+** (Add) button and specify the following details:

Configuration Parameters	Descriptions
Slice Number (applicable to Slice Mode)	Numerical value that represents the Slice ID. This value cannot be changed for Cisco NCS 1004 devices.
Client Bitrate	Total number of bits per second (in gigabits per second) to be configured on the client ports of the slice.
Trunk Bitrate	Total number of bits per second (in gigabits per second) to be configured on the trunk ports of the slice. **Note** When in **Regen Mode**, only the **Trunk Bitrate** is applicable for configuration.

Configuration Parameters	Descriptions
MAC Address Snooping	If enabled, it shows the neighboring MAC address. **Note** This option appears only for line card NCS1K4-1.2T and its variants.
LLDP Drop	When you enable the LLDP drop on the client controller ports of the muxponder, the LLDP frames drop on the ports without forwarding. **Note** This option appears only for line card NCS1K4-2-QDD-C-K9.

Step 6 Click **Save** to deploy the changes to the device immediately.

- For the types of line cards supported, see Supported Devices Tool
- For more information, see Cisco Network Convergence System 1000 Series.

Configure Line Card Operating Mode for Cisco NCS 1004 devices

To configure the NCS1K4-OTN-XP card operating mode for Cisco NCS 1004 devices and to activate or deactivate a line card:

Step 1 Launch the **Chassis View** as described in Open the Chassis View, on page 92.
Step 2 Click the **Configuration** tab from the window displayed on the right.
Step 3 Expand the **Line Card Operating Mode** subtab.
Step 4 To edit the line card operating mode, select the card operating mode and click **Edit**.
Step 5 Select the **Card Operating Mode** from the drop-down list and assign the desired action to it from the **Action** drop-down list.
Step 6 Click **Apply** to deploy the changes.

Configure Slices

Using Cisco EPN Manager you can configure the slice by controlling the bitrate on the client and trunk ports and by configuring the FEC and encryption types for each slice.

You must configure the five client ports of the slice at the same bitrate. Also, ensure that both trunk ports are always set to the same FEC mode.

Note Slice configuration is currently only supported for Cisco NCS 1002 and NCS 1004 devices.

Configure Slices for NCS 1002 Devices

To configure the slice for Cisco NCS 1002 device:

Step 1 Launch the **Chassis View** as described in Open the Chassis View, on page 92.

Step 2 Click the **Configuration** tab from the window displayed on the right.

Step 3 Expand the **Slice Configuration** sub-tab.

Step 4 To add new slice configuration, click the + (Add) button and specify the following details:

Slice Configuration Parameters	Descriptions
Slice Number	Numerical value that represents the Slice ID. You can create only one set of configuration per slice.
Client Bitrate	Total number of bits per second (in gigabits per second) to be configured on the client ports of the slice.
Trunk Bitrate	Total number of bits per second (in gigabits per second) to be configured on the trunk ports of the slice.
FEC	FEC value to be set on the trunk ports. Before changing the FEC mode setting, ensure that the admin state of the interface you are trying to modify is in Down (out of service) state with G709 configuration enabled.
Encryption	Configures the slice to function with encrypted or unencrypted traffic.

Step 5 Click **Apply** to deploy the changes to the device immediately.

You can add only one set of parameters per slice and not all parameters are editable once saved. To edit the parameters, delete the configuration for the slice and add it again.

Note The slice configuration cannot be deleted if the admin state is UP.

Configure Slices for NCS 1004 Devices

To configure the slice for NCS1004 devices:

Step 1 Launch the **Chassis View** as described in Open the Chassis View, on page 92.

Step 2 From the **Chassis Explorer**, select the slot that you want to configure.

Step 3 Click the **Configuration** tab from the window displayed on the right.

Step 4 Expand the **Slice Configuration** sub-tab.

Step 5 From the **Card Mode** drop-down list select the applicable option.

The available options are **Slice Mode**, **Muxponder Mode**, and **Regen Mode**.

Step 6 To add new slice configuration, click the + (Add) button and specify the following details:

Slice Configuration Parameters	Descriptions
Slice Number	Numerical value that represents the Slice ID. This value cannot be changed for NCS 1004 devices.
Client Bitrate	Total number of bits per second (in gigabits per second) to be configured on the client ports of the slice. The options available to select from are **100GE** and **OTU4**. **100GE** is applicable for both **Slice Mode** and **Muxponder Mode**. **OTU4** is only applicable for **Muxponder Mode**.
Trunk Bitrate	Total number of bits per second (in gigabits per second) to be configured on the trunk ports of the slice. **Note** When in **Regen Mode** the **Trunk Bitrate** is only applicable for configuration.
MAC Address Snooping	If enabled, it shows the neighboring MAC address.

Step 7 Click **Apply** to deploy the changes to the device immediately.

You can add only one set of parameters per slice and not all parameters are editable once saved. To edit the parameters, delete the configuration for the slice and add it again.

Note The slice configuration cannot be deleted if the admin state is UP.

Configure Interfaces from the Device Details Page

Complete the following procedure to configure an interface from the Device Details page:

Step 1 With a device's Chassis View open, click the **Launch Configuration** link. The Device Details page opens.

Step 2 Click the **Device Details** tab.

Step 3 From the **Features** pane, choose **Interfaces** > the interface type you want to configure.

Step 4 Complete the instructions specific to the interface type that you chose to add or edit an interface (see Configure Interfaces, on page 349).

Update Cisco NCS 1000 Interface Settings

You can quickly update the **Admin Status**, **Wavelength (nm)**, and **Loopback** settings for interfaces configured on a Cisco NCS 1000 Series device from its Device Details page. To do so, complete the following procedure.

Step 1 Open the Device Details page for a Cisco NCS 1000 Series device, as described in Get Complete Device Information: Device Details Page, on page 90.

Step 2 Click the **Configuration** tab.

The page updates, displaying 3 sub-tabs: **Optics**, **Ethernet**, and **Coherent DSP**.

Step 3 Click the sub-tab for the interface type you want to update.

Step 4 Make the necessary changes:

Method 1

a. In the interfaces table, locate the interface you want to update.

b. Click the parameter you want to change to open a drop-down list.

c. Choose the value you want to set, then click **Save**.

Method 2

a. Click the radio button for the interface you want to update, then click the pencil (**Edit**) icon.

The **Edit** *interface type* dialog box opens.

b. Choose the value you want to set from the available drop-down lists, then click **Apply**.

c. Click **OK** to confirm your changes.

Note the following:

- For Optics interfaces:
  - You can update the **Admin Status** and **Wavelength (nm)** parameters.
  - You can only set a new wavelength value if the **Optics Type** parameter is set to **DWDM**.
- For Coherent DSP and Ethernet interfaces:
  - You can update the **Admin Status** and **Loopback** parameters.
  - You can only set a new loopback value if the **Admin Status** parameter is set to **Testing**.
  - If you set the **Loopback** parameter to **Line**, Cisco EPN Manager applies the same configuration applied for a facility loopback. A facility loopback tests the line interface unit (LIU) of a card, the electrical interface assembly (EIA), and related cabling.
  - If you set the **Loopback** parameter to **Internal**, Cisco EPN Manager applies the same configuration applied for a terminal loopback.

Configure Controllers (Optics, OTS, OCH, DSP, and DWDM)

Using Cisco EPN Manager, you can configure optical device controller parameters such as the wavelength, FEC, SD, and SF BER reporting and thresholds, and more for controllers of type OTS, OTS OCH, DWDM, and more.

The Optical Transport Section (OTS) controller holds all the optical parameters for the OTS optical interfaces. The optical interface has different capabilities depending on its hardware components such as VOA and amplifier. Hence, the parameters that are enabled or disabled on the OTS controller depend on the actual hardware capability on the specific optical interface. You can configure parameters such as amplifier gain range, amplifier tilt, and optical safety remote interlock (OSRI) for the OTS controller.

The Optical Transport Section OCH (OTS OCH) controller represents the OCM device available on the OTS optical interface. This controller has channel granularity over the OTS interface. The OTS OCH controller contains the wavelength information. You can configure only the admin status for the OTS OCH controller.

To ensure that you complete the slice configuration before configuring the controllers, see, Configure Slices for NCS 1002 Devices, on page 381.

To configure the optical controller parameters:

Step 1 Launch the **Chassis View** as described in Open the Chassis View, on page 92.

Step 2 Click the **Configuration** tab from the window displayed on the right.

Step 3 Expand the **Controllers** subtab. Depending on your device selection, supported tabs are displayed.

Step 4 To edit the configuration on optical controllers, click **Optics**, choose the required settings, and click the modify icon to make your changes.

Step 5 To edit the configuration on OTS controllers, click **OTS**, choose the required settings, and click the modify icon to make your changes.

Step 6 To edit the configuration on OTS-OCH controllers, click **Ots-Och**, choose the required settings, and click the modify icon to make your changes.

Step 7 To configure coherent DSPs, click **Coherent DSPs**, choose the required settings, and click the modify icon to make your changes.

Note You cannot edit any parameter when the transport admin status is set to IS.

Step 8 To edit the configuration on DWDM controllers, click **DWDM**, choose the required settings, and click the modify icon to make your changes.

Category	Parameters	Description
Common Optics, OTS-OCH, DSP, and DWDM Controller Parameters	• Name • Admin Status • Operational Status • Transport Admin Status	Name- (Display only) Displays the port number. Admin Status-Defines whether the interface is managed (Up), down, or in maintenance mode. You cannot modify the controller properties when the status of the interface is Up. Operational Status – Defines whether the interface is operational and is performing as provisioned. Transport Admin Status – Defines the transport administration state of the controller.
Common Optics and DWDM Parameters	• Actual Wavelength (nm) or Actual Frequency (thz) • Wavelength (nm) or Frequency (thz)	Displays the wavelength and frequency utilized by the channel.
-	Wavelength (nm)	Displays the wavelength value configured on the channel. Once the device Inventory Collection status is completed, the Actual Wavelength and Wavelength values match.
-	FEC Mode	FEC value to be set on the controllers.

Category	Parameters	Description
		Before changing the FEC mode setting, ensure that the admin state of the interface you are trying to modify is in Down (out of service) state with G709 configuration enabled.
Optics Parameters	Speed	Set the speed values (in gigabits per second) that the controllers must operate on.
-	DAC Rate	Select the DAC rate from the drop-down list.
-	Min Chromatic Dispersion	Enter the minimum chromatic dispersion value.
-	Max Chromatic Dispersion	Enter the maximum chromatic dispersion value.
-	Configured Tx Power	Enter the transmit power.
-	Modulation Type	Set the modulation type from the drop-down list.
-	Differential Modulation	Enable or disable Differential Encoding (DE) based on the configured speed values.
-	Loopback	Configure the loopback as: • Internal - All packets are looped back internally within the router before reaching an external interface. It tests the internal Rx to Tx path and stops the traffic to egress out from the Physical port. • Line - Incoming network packets are looped back through the external interface.
-	SD BER	Set the signal degrade bit error rate. Your options are E-5, E-6, E-7, E-8, or E-9.
-	SF BER	Set the signal fail bit error rate. Your options are E-3, E-4, or E-5.
DWDM Parameters	Loopback	Configure the loopback as: • Internal - All packets are looped back internally within the router before reaching an external interface. It tests the internal Rx to Tx path and stops the traffic to egress out from the Physical port. • Line - Incoming network packets are looped back through the external interface.
-	• OTU-SD • OTU-SF • ODU-SD • ODU-SF	Configure SF (signal fail) and SD (signal degrade) BER reporting and thresholds. Depending on whether the alarm is an OTU or ODU alarm, the alarm represents that SM BER is in excess based on the SD BER threshold or SF BER threshold.
OTS Parameters	Port Role	Current operational state of the port.

Category	Parameters	Description
		For a protection switch, the Com work role is displayed, whereas, for an amplifier module, the Com Line/Osc or Com Check role is displayed.
-	Rx/Tx Low Threshold (dBm)	Configures the receiver/transponder low receive power threshold. The valid range is from -500 to 300.
-	Ampli Channel Power (dBm)	Configures the amplifier per channel power set point. The valid range is -500 to 300. The default value is 0.0.
-	Channel Power Max Delta (dBm)	Configures the maximum difference among all the measured channel powers. The valid range is 0–200.
-	Ampli Gain and Ampli Gain Range	Configures the amplifier gain set point. The valid mode for the range is normal or extended. **Note** The amplifier gain range is configurable only when the controller is in shutdown state.
-	Ampli Safety Controller Mode	Configures the safety control mode as auto or disabled.
-	OSRI	Configures the optical safety remote interlock as on or off.
-	Ampli Tilt	Configures the amplifier tilt using a number between -50 to +50.

Note The values you see in IOS-XR (RON) optical controller edit screen, is the running configuration on the device.

When **Not Set** is selected for Optics Controller DAC Rate, FEC and Modulation Type attributes, EPNM removes the existing configuration from device and it shows the operational value of those attributes on the user interface once GI completes.

Step 9 Click **Apply** to deploy your changes to the device immediately.

Step 10 (Optional) To change the unit of the DWDM grid value to either wavelength or frequency, go to **Administrator > Settings > System Settings > Circuits/VCs**, and under the DWDM Grid Unit area, choose either **Wavelength (Nanometer (nm))** or **Frequency (Tatrahertx (THz)).**

Configure Passive Units

Passive units are passive cards provisioned using Cisco EPN Manager for optical devices. Cisco EPN Manager maintains these passive units in its database and does not deploy them to devices. Once configured, you can view these passive units in the Device Details and Inventory pages and use them to create managed links in the Network Topology.

Note Passive Unit configuration is currently only supported for Cisco NCS 1001 device.

To add and delete passive units:

Before you begin

Ensure that you have either 'Administrator' or 'Config Manager' user privilege before you perform this task.

Step 1 Launch the **Chassis View** as described in Open the Chassis View, on page 92.

Step 2 Click the **Configuration** tab from the window displayed on the right.

Step 3 Expand the **Passive Units** sub-tab.

Step 4 To add a passive unit click the Add (+) icon and specify the following details:

- Equipment ID: Choose the unique identifier for the passive unit. You can add up to 9 passive units per device.
- Equipment Type: Choose the equipment type that determines if the slot is provisioned as a 48-channel muxponder/demuxponder or as an odd/even unit. Your options are **CME**, **ODDE**, and **EVENE**.
- (Optional) Serial Number: Serial number that is unique to each passive unit. Cisco EPN Manager does not deploy this configuration to the device and maintains it only in its database.

Step 5 Click **Apply** to deploy your changes to the device.

Step 6 (Optional) To verify successful creation of the passive units, navigate to the Interfaces tab or to the Device Details tab and use the Interface Name filter to locate the passive units.

The naming convention used for the passive units is:

PUnit<number of the card> <equipment ID of the passive unit>

For example, *PUnit/1/16*.

Step 7 To edit the configuration of the passive units delete them and configure the details again using the same equipment ID.

Step 8 To delete the passive units, select the required passive unit and click the Delete (X) icon. Passive units associated with links can also be deleted. This causes the links to switch to the Partial state.

Step 9 (Optional) To match multiple passive units with same values, select the required passive unit and click **Match**. Select the simulated passive unit number from the dropdown list and click **Apply**.

Step 10 (Optional) To configure manual links using these passive ports, navigate to the network topology and create the links as described in Manually Add Links to the Topology Map, on page 180.

Edit Amplifier Module Settings on Optical Cards

You can modify the settings of amplifier modules inserted in optical slots of your device by changing the grid modes, node types, and UDC Vlan settings.

To edit the amplifier module settings:

Before you begin

Ensure that you have either 'Administrator' or 'Config Manager' user privilege before you perform this task.

Step 1 Launch the **Chassis View** as described in Open the Chassis View, on page 92.

Step 2 Click the **Configuration** tab from the window displayed on the right.

Step 3 Expand the **Amplifier Module Settings** sub-tab.

Step 4 Select the settings that you want to edit, click the Edit icon, and specify the following parameters:

- Grid Mode: Defines the optical spectrum on the interfaces of the amplifier module.
- Node Type: Defines the type of the node in which the amplifier is set to work. Your options are: Terminal, Line, and Not Set.
- Udc Vlan: Defines the VLAN associated to the selected slot and its UDC port.

Note Ensure that the Udc Vlan that you specify is unique on the device. Duplicate values are not supported.

Step 5 Click **Apply** to deploy your changes to the device.

Step 6 (Optional) To configure the Ethernet Controllers, expand the **Ethernet** sub-tab. Select the controller that you want to edit, click the Edit icon, and make the required changes. Click **Apply** to save the changes to the device.

Configure GMPLS and WSON Properties

GMPLS UNIs:

The Generalized Multiprotocol Label Switching (GMPLS) User Network Interface (UNI) creates a circuit connection between two clients (UNI-C) of an optical network. This connection is achieved by signal exchanges between UNI Client (UNI-C) and UNI Network (UNI-N) nodes, where UNI-C nodes are router nodes and UNI-N nodes are optical nodes.

GMPLS UNI is supported only on the 100G and 200G trunk ports of the Cisco NCS 1002 node. The prerequisite for the OCH trail circuit is to create a Link Management Protocol (LMP) link between the optical channel Add/Drop NCS 2000 series interface on the NCS 2000 series node and the NCS 1002 interface on the NCS 1002 node.

UNI is divided into client (UNI-C) and network (UNI-N) roles. A UNI-C network element requests and accepts the circuit provisioning information. A UNI-N network element is the node that is adjacent to the UNI-C node and accepts and transports circuit provisioning information across the core network.

For UNI circuit provisioning, the network must meet the following requirements:

- An NE must be configured in as UNI-C and connected to a UNI-N NE.
- An NE must be configured as UNI-N and connected to a UNI-C NE.

Static UNIs:

Link Management Protocol (LMP) is a logical link that is created on the trunk optics controller on the source and destination nodes of the tunnel. You can create static LMP links (Static UNIs) between the ports of two different devices. For example, between a Cisco NCS 2000 series node and a Cisco NCS 1002 node. This helps to configure an LMP neighbor for a GMPLS UNI tunnel.

While configuring a Static UNI using Cisco EPN Manager, choose the RX Port and TX Port, and identify the card, shelf, or slot that you want to engage in the UNI. While the RX Port represents the source for the UNI, the TX Port represents the destination.

Use the Remote Device field to specify the management IP address of the selected node. Use the Remote Client Interface field to choose the LMP link IP address of the optics controller.

Alien Wavelength:

Use the Alien Wavelength tab to view and configure the port and wavelength parameters of the alien wavelength. You can also specify the required alien wavelength type, trunk mode, and the forward error correction (FEC) mode.

Fiber Attributes:

You can configure the parameters that are used during the creation of the GMPLS UNI by configuring values such as the fiber type (by choosing Dispersion-Shifted (DS), True-Wave Classic (TWC), or other values). You can also specify the fiber length and specify the Polarization Mode Dispersion fiber coefficient.

The Attenuator In value identifies the input optical attenuation in dB between the node output port (for example, a LINE-TX port) and the input parameter of the fiber. Similarly, the Attenuator Out value identifies the same between the node input port (for example, a LINE-RX port) and the output parameter of the fiber.

You can choose the Channel Spacing value that configures the minimum frequency spacing between two adjacent channels in the optical grid. To specify the maximum number of channels that are expected on the span use the Channel Number field, ensure that the channel number and channel spacing values are consistent. For example, there cannot be 80 channels with 100-GHz spacing.

Virtual Trunk:

You can use the Virtual Trunk tab to specify the Drop Ports, Description Configuration, TXP Control Mode, and Alien Wavelength Type for the device.

LMP Termination:

You can use the LMP Termination tab to specify the Virtual Trunk, LMP Type, Remote Device, Remote Interface, and Peering for a device. You can also edit the existing LMP Terminations in the LMP Termination tab.

To configure GMPLS/WSON parameters:

Step 1 Launch the **Chassis View** as described in Open the Chassis View, on page 92.

Step 2 Click the **Configuration** tab from the window that is displayed on the right.

Step 3 To configure these parameters, navigate to the paths described in the table below:

Task	Navigation	Description
Configure fiber attributes	GMPLS/WSON sub-tab > Fiber Attributes	Specify the fiber side, type, length, validation, channel spacing, channel number, and domain values. You can also specify the attenuator (in and out) values (optional).
Create and edit static UNIs	GMPLS/WSON sub-tab > Static UNIs	• Add the RX and TX port remote controllers that must participate in the UNI. • The Remote Device field specifies the management IP address of the node. • The Remote Client Interface field specifies the link IP address of the controller. **Note** You can configure a remote TXP node using the above settings.
Create and edit GMPLS UNIs	GMPLS/WSON sub-tab > GMPLS UNIs	• Specify the ingress and egress ports for the GMPLS UNI and choose if the UNI is of numbered or unnumbered type. Ensure that you specify if the UNI is of type UNI-C or UNI-N.

Task	Navigation	Description
		• The trunk values are automatically configured to the respective alien wavelength values depending on your GMPLS UNI configuration. If the configured alien wavelength is supported on both trunk ports, then setting it on one of the trunk ports automatically configures the same alien wavelength on both trunk ports. • For Cisco NCS 2000 devices, the GMPLS UNI trunk value can be set to Default. • Specify the local and remote interface IP, and remote system IP and controller. These values enable the remote system connection for the UNI. **Note** You can only specify remote system IPs of devices that are managed by Cisco EPN Manager.
Configure Alien Wavelength parameters	GMPLS/WSON sub-tab > Alien Wavelength	Specify the required alien wavelength type, trunk mode, and the FEC mode.
Configure and Edit Virtual Trunk	GMPLS/WSON sub-tab > Virtual Trunk	Specify the Drop Ports, Description Configuration, Txp Control Mode (LOCAL and NONE), and Alien Wavelength Type. **Note** You can only edit the description and not any other attributes.
Configure and Edit LMP Termination	GMPLS/WSON sub-tab > LMP Termination	Specify the Virtual Trunk, LMP Type, Remote Device, Remote Interface, and Peering. **Note** If a NCS2K device has an LMP Type as **NoSignal** and TXPCONTROLMODE as **GMPLS**, then **Signaled (NCS1004)** appears as the LMP type (discovered LMP) in the EPNM UI (in cases of NCS2K to NCS1004 LMP or NCS2K to NCS4K LMP).

Note For a Not-Signaled LMP, the commands will be pushed only on the local device. You have to push the configuration either manually or using a configuration template to the remote device.

Step 4 Make your changes and click **Save**.

Step 5 To edit the values once configured, select the values and click the Edit icon in the toolbar. Make your changes and click **Save**.

For information on LMP link creation, see, Optical Channel (OCH) Trail User-to-Network Interface (UNI), on page 488.

Enable or Disable Optical Safety Remote Interlock (OSRI) on OTS Ports

You can modify the optical safety remote interlock (OSRI) status for the configured ports on OTS interfaces.

To enable or disable OSRI:

Before you begin

Ensure that you have either 'Administrator' or 'Config Manager' user privilege before you perform this task.

Step 1 Launch the **Chassis View** as described in Open the Chassis View, on page 92.

Step 2 Click the **Configuration** tab from the window displayed on the right.

Step 3 Expand the **Maintenance** tab and click the **OSRI** sub tab.

Step 4 Select the port for which you want to enable or disable the OSRI.

Step 5 From the drop-down list, select **Enable** or **Disable** to enable or disable the OSRI.

Perform a Chassis Level Reset/Reload

Reset/reload a device on the chassis level. Cisco EPN Manager does not modify any configuration changes, instead saves the settings, and triggers an inventory collection.

To reload a device:

Step 1 Launch the Device 360 view for the device as described in Get Basic Device Information: Device 360 View, on page 84.

Step 2 From the **Actions** drop-down, choose the **Reset** option. A pop-up warning window appears asking you to confirm your action, click **Yes** to proceed.

Note The **Reset** feature is not available for Cisco NCS 2000 series, Cisco NCS 1000 series, and Cisco NCS 4000 series devices.

Configure Optical Cards

Configure Cards from the Chassis View

This procedure adds a card to Cisco EPN Manager using the Chassis View. After adding the card, you can configure it by following the procedure in the relevant topic for that card type. Normally this is done before you physically add the card to the slot.

Before you begin

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

Step 1 Launch the Chassis View as described in Open the Chassis View, on page 92.

Step 2 Select the slot to which you want to add the card by following one of the steps given below:

- Select the empty slot from the physical Chassis View, then click the **Add Card** link in the slot pop-up window.
- Use the Chassis View explorer to navigate to the empty slot, hover your mouse cursor over the "i" icon next to the slot, then click the **Add Card** hyperlink in the informational popup window.

Cisco EPN Manager highlights the slot in the physical Chassis View (indicating that it is preprovisioned) and lists all of the cards that are supported by that device type.

Note Make sure the card that you select is appropriate for the physical slot type.

Step 3 Locate the card that you want to add, then click **Add**. Cisco EPN Manager displays a status message after the card is added.

Step 4 If you want to configure the card right away, click **Configure Now** in the status popup message. Otherwise, click **Ignore**.

Delete a Card

When you delete a card, Cisco EPN Manager removes all information about the card including the card operating mode configuration associated with the card. When you add this card again at a later point of time, this information is not restored.

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

To delete a card from Cisco EPN Manager:

Before you begin

Before you delete a card, make sure that:

- The associated payload values and card operating modes are deleted.
- The card does not have any active configuration running on the card (you will not able to restore the configuration when you re-add the card).

Step 1 Launch the Chassis View as described in Open the Chassis View, on page 92.

Step 2 Select the slot from which you want to delete the card by doing one of the follow:

- Select the card in the slot from the physical Chassis View, then click the **Delete Card** link in the pop-up window.

- Use the Chassis View explorer to navigate to the card, hover your mouse cursor over the "i" icon next to the card, then click the **Delete Card** hyperlink in the popup window.

Cisco EPN Manager highlights the slot in the physical Chassis View (indicating it is pre-provisioned) and once you delete all cards of a slot, the slot is left blank in the Chassis View.

After you delete a card, Cisco EPN Manager performs an inventory collection for the node.

Reset a Line Card

Resetting a line card repositions and resets the card in the chassis. Cisco EPN Manager does not modify any configuration changes, instead saves the settings, and triggers an inventory collection.

To reset a configured card:

Step 1 Launch the Chassis View as described in Open the Chassis View, on page 92.

Step 2 Select the slot from which you want to reset the card using one of the following procedures:

- Select the card in the slot from the physical Chassis View, then click the **Reset** hyperlink in the pop-up window.
- Use the Chassis View explorer to navigate to the card, hover your mouse cursor over the "**i**" icon next to the card, then click the **Reset** hyperlink in the pop-up window.

Cisco EPN Manager highlights the slot in the physical Chassis View (indicating that it is preprovisioned). After you reset the card, a sync is performed, and an inventory collection is triggered.

Note The **Reset** feature is unavailable for Cisco NCS 2000 series, Cisco NCS 1000 series, and Cisco NCS 4000 series devices.

Cisco NCS 2000 series devices have the reset function for preprovisioned cards only.

What to do next

Configure the properties of the card as described in Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC, on page 395.

Configure cards: OTU2-XP, MR-MXP, WSE, AR-XPE, AR-XP, AR-MXP, 40E-MXP-C, and 40ME-MXP-C

To configure card operating modes and Pluggable Port Modules (PPMs):

Before you begin

OTU2-XP and 40E-MXP-C cards can be configured with PPM directly without having to set the card operating mode. However, if you want to configure card operating modes for other cards you can perform this configuration directly via Cisco Transport Controller.

- Ensure that the device sync is complete and that the device's inventory collection status is 'Managed' or 'Completed'.
- Every time you add or delete a PPM, reactive inventory collection is triggered, and the device begins the sync process. Ensure that you wait for reactive inventory collection to complete before you deploy further configuration changes to the device. When the device sync is in progress, the deploy of PPM configuration changes to the device will fail.
- Once the card operating modes are configured, ensure that the device sync is completed. If not, Cisco EPN Manager will not be able to display the right Payload values for the selected cards.
- Ensure that granular inventory is enabled for all cards before performing any configuration changes on the cards.
- For all supported cards except 40E-MXP-C, 40ME-MXP-C, and OTU2-XP cards, you must first configure the card operating modes using Cisco Transport Controller and then return to Cisco EPN Manager to proceed with the following steps.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device's Name hyperlink to launch the device's Chassis view. This feature is supported only on Cisco NCS 2000 devices.

Step 3 Use the **Chassis Explorer** to select the card that you want to configure.

Step 4 Click the **Configuration** sub-tab from the window displayed on the right.

Step 5 Navigate to the CTC tool and configure the operating modes for the cards. Card mode configuration is not supported on: OTU2-XP, MR-MXP, WSE, AR-XPE, AR-XP, and AR-MXP cards. For all other cards on Cisco NCS 2000 devices, configure card operating modes as described in Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC, on page 395.

Step 6 Expand the **Pluggable Port Modules** section to configure port modules and their respective payload values.

Step 7 Click the '+' (Add) icon in the **Port Modules** section to create port modules (PPMs).

Step 8 Select the **PPM number** and then click **Save**. The PPM port is set to PPM (1 port) by default and cannot be modified.

Note The '+' (Add) button is disabled when the maximum number of PPMs for the selected card are created. You must create all available ports before you can continue to the next step.

Step 9 Click the '+' (Add) icon in the **Pluggable Port Modules** section.

Note For some PPMs, the respective payload values may not be enabled. To enable it, complete the card mode configuration described in Step 5 above, and then try to re-configure the payload values.

Step 10 Choose the **port number**, **port type**, and **number of lanes** that must be associated with the selected PPM. The Port Type (payload) can be set to any supported client signals described in Table 2 below.

Note If the specified Port Type (payload) is not supported for the selected card operating mode or PPM, then the changes are not deployed to the device successfully. Ensure that the Payload values you specify, are supported on the selected card. See Table 2 below for reference.

Step 11 Click **Finish** to deploy your changes to the device.

Step 12 (Optional) If your changes are not visible in the Cisco EPN Manager, it could be because more than one person is working on the same card mode configuration and the changes are not reflected dynamically. Click the Refresh icon within each section to view the most recent changes.

If you encounter a deploy failure, navigate to the error logs folder **/opt/CSCOlumos/logs/config.log** for more details about the cause of the error.

Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC

To configure card operating modes and PPMs:

Before you begin

- Ensure that the device sync is complete and that the device's inventory collection status is 'Completed'. If the device sync is on, then the deploy of PPM configuration changes will fail.
- Card mode configuration is not supported on: OTU2-XP, MR-MXP, WSE, AR-XPE, AR-XP, and AR-MXP cards. To configure the card operating modes on these cards, please use the Cisco Transport Controller tool.
- Ensure that the device sync is complete and that the device's inventory collection status is 'Managed' or 'Completed'.
- Ensure that granular inventory is enabled for all cards before performing any configuration changes on the cards.
- By default, device throttling is not enabled. To enable device throttling, navigate to **cd /opt/CSCOlumos/xmp_inventory/xde-home/inventoryDefaults** and execute **vi onsTL1.def** and add the following xml tag:

  <default attribute="DEVICE_THROTTLING">noOfconnections</default>

  Here, **noOfconnections** is number of the max TL1 session to the EPNM.

  For example: **<default attribute="DEVICE_THROTTLING">6</default>**

Step 1 Choose **Configuration** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device's Name hyperlink to launch the device's Chassis view.

Step 3 Use the **Chassis Explorer** to select the card that you want to configure.

Step 4 Click the **Configuration** sub-tab from the window displayed on the right.

Step 5 Expand the **Pluggable Port Modules** section to configure port modules and their respective payload values.

Step 6 Click the '+' (Add) icon in the **Port Modules** section to create port modules (PPMs). Select the PPM number and then click **Save**. The **PPM Port** value is set to PPM (1 port) by default and cannot be modified.

Note

- The '+' (Add) button is disabled when the maximum number of PPMs applicable for the selected card are created. You must create the required number of PPMs for the selected card before proceeding to the next step. For 100G-CK-C cards, you only need to create at least one PPM before proceeding to the next step.
- For 400G-XP-LC cards, ensure that the PPMs 11 and 12 are created before configuring the card operating modes described in the next step (although the card mode is being created for either of the trunk ports). Without PPMs 11 and 12, the configuration changes deployed to the device will fail.
- This step is optional for 100G-LC-C, 100G-ME-C, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, and 100GS-CK-C cards.

Step 7 Expand the **Card Operating Modes** section to configure operating modes for the selected card.

Step 8 Click the '+' (Add) icon to display a list of supported card operating modes or click the Edit icon to modify existing card operating modes. For 10x10G-LC cards you can add up to 5 card operating modes (10 ports that can act as sets of client or trunk ports), whereas for all other cards, only a single card operating mode can be set, after which, the + (Add) button is disabled.

Step 9 Select an operating mode from the panel on the left and make your changes to the parameters.

Note

- Some card operating modes are disabled based on the card's peer configuration. Click on the '**i**' icon next to the operating modes to understand how they can be enabled. See Table 1 below to understand the peer card configuration required to enable these operating modes.
- For MXP cards, ensure that the trunk, peer, and peer skip card configuration is in the order described below:

Card Operating Modes	Trunk Card	Peer Card	Peer Skip Card
MXP_200G	Slot 2	Slot 3	Slot 4
MXP_200G on ONS 15454 M6 devices	100GS-CK-LC or 200G-CK-LC card in slots 2 or 7.	Slots 3, 4 or 5, 6.	Slots 3, 4 or 5, 6.
MXP_200G on Cisco NCS 2015 devices	100GS-CK-LC or 200G-CK-LC card in slots 2, 7, 8, 13, or 14.	MR-MXP cards in adjacent slots.	MR-MXP cards in adjacent slots.
MXP_10x10G_100G	Slot 7	Slot 6	Slot 5
MXP_10x10G_100G on ONS 15454 M6 devices	100GS-CK-LC or 200G-CK-LC card in slots 2 or 7	MR-MXP cards in adjacent slots 3, 4 or 5, 6.	MR-MXP cards in adjacent slots 3, 4 or 5, 6.
MXP_10x10G_100G on Cisco NCS 2015 devices	100GS-CK-LC or 200G-CK-LC card in slots 2, 7, 8, 13, or 14.	MR-MXP cards in adjacent slots.	MR-MXP cards in adjacent slots.
MXP_CK_100G on ONS 15454 M6 devices	100GS-CK-LC or 200G-CK-LC card and the peer MR-MXP card need to be in adjacent slots 2-3, 4-5, 6-7.		
MXP_CK_100G on Cisco NCS 2015 devices	100GS-CK-LC or 200G-CK-LC card and the peer MR-MXP card need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.		

For 400G-XP-LC cards, you can configure the OTNXC card operating mode with trunk operating mode of M-100G/M-200G. Based on the trunk operating mode, the supported slice configuration (either "Slice 1 and Slice 4" or slice 1, 2, 3, 4 respectively) are OPM-100G and OPM-10x10G.

The trunk operating mode configured on the trunk 11 reflects automatically in the trunk 12. For example, when you configure M-200G on trunk 11, the trunk operating mode for trunk 12 will be greyed out; However, M-200G will be automatically configured on trunk 12. It is possible to mix OPM_100G slices with OPM_10x10G slices, and each slice will be independent.

Step 10 Click **Save** to deploy your changes to the device.

Step 11 Expand the **Pluggable Port Modules** section to configure the payload values for each PPM.

Step 12 Click the '+' (Add) icon in the Pluggable Port Modules section.

Note For some PPMs, the respective payload values may not be enabled. To enable it, complete the card mode configuration described in Step 9 above, and then try to re-configure the payload values.

Step 13 Choose the **port number**, **port type**, and the **number of lanes** that must be associated with the selected PPM. The Port Type (payload) can be set to any supported client signals described in the Table 1 below.

Note
- If the specified Port Type (payload) is not supported for the selected card mode or PPM, then the changes are not deployed to the device successfully. Ensure that the Payload values you specify, are supported on the selected card. See Table 1 for reference.
- You can configure the number of lanes only on cards that allow payload values to be split. For all other cards, the Number of Lanes field is disabled.

Step 14 Click **Finish** to deploy your changes to the device.

Step 15 (Optional) If your changes are not visible in the Cisco EPN Manager, it could be because more than one person is working on the same card mode configuration and the changes are not reflected dynamically. Click the Refresh icon within each section to view the most recent changes.

If you encounter a deploy failure, navigate to the error logs folder **/opt/CSCOlumos/logs/config.log** for more details about the cause of the error.

Configure SONET and Flex Line Cards

This procedure describes how you can use Cisco EPN Manager to modify the line card configuration on 10X10G-LC SONET cards and 400G-XP, 200G-CK-LC, and 100GS-CK-LC Flex cards.

This feature is only supported on Cisco NCS 2000 and Cisco ONS devices.

To configure a SONET or Flex line card:

Before you begin

- To configure SONET line cards, ensure that you select a card with the operating mode MXP10X10G and OC192 payload value.
- To delete the SONET or Flex line card configuration, you only need to delete the payload values associated with the selected card. This deletes the SONET or Flex configuration from the device automatically. To delete the payload values, use the Pluggable Port Modes area under the configuration sub-tab.
- While configuring the SONET or Flex line card configuration, if you want to change the Line card type from SONET to SDH, or make other similar changes, you must first ensure that the admin state of the device is set to OOS-Disabled. If the device state is not OOS-Disabled, the line configuration changes deployed to the device will fail.
- To configuring Flex line card configuration, ensure that the card operating modes for the card have been previously set. See Configure cards: 400G-XP-LC, 100G-CK-C, 100ME-CK-C, 200G-CK-LC, 100GS-CK-C, 100G-LC-C, 100G-ME-C, and 10x10G-LC, on page 395.

Step 1 Launch the Chassis View as described in Open the Chassis View, on page 92.

Step 2 Select the slot from which you want to configure the card by doing one of the follow:

- Select the card in the slot from the physical Chassis View using the zoom in and out options.
- Use the Chassis Explorer view to navigate to the card and select it.

Step 3 Click the **Configuration** sub-tab from the window displayed on the right.

Step 4 Expand the **Line** section and choose the **SONET** or **Flex** sub-tabs.

The supported cards for SONET configuration are only 10x10G-LC cards, and for Flex cards, it is 400G-XP, 200G-CK-LC, and 100GS-CK-LC cards.

Step 5 Choose one of the following ways to edit the configuration:

- Select the SONET or Flex tab for configuration that you want to edit and click the Edit icon.
- Click the inline parameters that you want to edit one by one within the rows of the table.

Step 6 Make the required changes to the parameters described in the table below and click **Save** to deploy your changes to the device.

While configuring SONET parameters:

- When you set the Type to SDH, the Sync Messages checkbox is automatically disabled and cannot be configured.
- When you enabled the Sync Message checkbox, the Admin SSM option is disabled and set to null.

While configuring Flex parameters:

- For 400G-XP-LC cards, Flex line cards can be configured only for trunk ports 11/12.
- For 100GS-CK-LC cards, Flex line cards can be configured only for trunk port 2.

Table 24: SONET and Flex Line Configuration Parameters and Descriptions

Line Card Type	Line Card Configuration Parameters	Descriptions
SONET	Port Number	The port number of the SONET interface you are configuring.
	Port Name	Allows you to add a name for the SONET optical port.
	SD BER	Sets the signal degrade bit error rate.
	SF BER	Sets the signal fail bit error rate.
	Type	Defines the port as SONET or SDH.
	Provides Sync	When checked, the card is provisioned as an NE timing reference.
	Sync Messaging	Enables synchronization status messages (S1 byte), which allow the node to choose the best timing source.
	Admin SSM In	If the node does not receive an SSM signal, it defaults to synchronization traceability unknown (STU). Admin SSM allows you to override the STU value with one of the following: • PRS—Primary reference source (Stratum 1) • STS2—Stratum 2 • TNC—Transit node clock • STS3E—Stratum 3E • STS3—Stratum 3 • SMC—SONET minimum clock • ST4—Stratum 4
Flex	Port	The port number of the Flex interface you are configuring.
	Gridless	Enables or disables the gridless tunability feature on the selected card. When the feature is enabled, you can configure the frequency values on the card. Your options are: • Enabled- When selected, enables you to edit the frequency parameter for Flex. • Disabled- When selected, disables the frequency parameter for Flex.
	Frequency	Specifies the frequency on the port of the 400G-XP, 200G-CK-LC, and 100GS-CK-LC cards in the range 191350 to 196100.

Edit and Delete Pluggable Port Modules and Card Mode Configuration

Before you begin

Pre-requisites for deleting PPMs:

- Ensure that the PPMs are not part of any Active or Provisioned circuits.
- PPMs and their respective payload values must be deleted only in the order described in the procedure below. Ensure that you first manually delete client ports 1 to 10 before deleting associated PPMs.
- Ensure that device sync is completed and the device's inventory collection status is either 'Completed' or 'Managed'.

Pre-requisite for deleting card operating modes:

- Ensure that the cards are not part of any Active or Provisioned circuits.
- For 400G-XP cards, PPMs 11 and 12 cannot be deleted. These PPMs are deleted automatically when the associated card operating mode is deleted.
- The peer card or skip card must not be in Active state. You can delete the peer or skip card associations using CTC and then retry deleting the card operating mode via Cisco EPN Manager. You can also try directly deleting the card from Cisco EPN Manager. For more information, see Delete a Card, on page 392.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device's Name hyperlink to launch the device's Chassis view.

Step 3 Use the **Chassis Explorer** to select the card with the configuration you want to delete.

Step 4 Click the **Configuration** sub-tab from the window displayed on the right.

Step 5 Expand the **Pluggable Port Modules** section to delete Pluggable Port Modules (PPMs).

a) In the **Pluggable Port Modules** sub-section, select the associated payload values that you want to delete and click the '**X**' (delete) icon.
b) Click **OK** to confirm. The changes are deployed to the device.
c) In the **Port Modules** sub-section, select the PPMs that you want to delete and click the '**X**' (delete) icon.
d) Click **OK** to confirm. The changes are deployed to the device.

Note You must delete all payload values associated with a given PPM, before you can delete the PPM.

Step 6 Expand the **Card Operating Modes** section to delete the card configuration.

a) To edit the card mode configuration, ensure that you select only 400G-XP cards, and click the Edit icon to make your changes. For all other cards, the configuration can be edited only by deleting the card mode configuration and re-creating it with new values.
b) To delete the card mode configuration, select the required card mode configuration and click the '**X**' (delete) icon.
c) Click **OK** to confirm. The changes are deployed to the device.

Cards and Supported Configuration for Cisco NCS 2000 Devices

Table 25: 100GS-CK-LC and 200G-CK-LC Cards: Supported Configuration

Card Operating Modes	Trunk Card	Peer card	Peer Skip Card	Supported Payload Types
MXP_200G	100GS-CK-LC or 200G-CK-LC card in slots 2, 7, 8, 13, or 14.	MR-MXP cards in slots 3, 6, 9, 12 or 15.	MR-MXP cards in slots 4, 5, 10, 11 or 16.	100GE and OTU4 OTU4 is supported only for the 200G-CK-LC card. Regeneration of any 100 G configuration 10GE 10GE 100GE
MXP_10x10G_100G	100GS-CK-LC or 200G-CK-LC card in slots 2, 7, 8, 13, or 14.	10x10G-LC cards in slots 3, 6, 9, 12 or 15.	MR-MXP cards in slots 4, 5, 10, 11 or 16.	100GE and OTU4 OTU4 is supported only for the 200G-CK-LC card. Regeneration of any 100 G configuration 10GE 10GE 100GE
MXP_CK_100G	100GS-CK-LC or 200G-CK-LC card and the peer MR-MXP card need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.	N/A	N/A	100GE and OTU4 OTU4 is supported only for the 200G-CK-LC card. Regeneration of any 100 G configuration 10GE 10GE 100GE
RGN-100G	100GS-CK-LC or 200G-CK-LC card and the peer card 100GS-CK-LC or 200G-CK-LC need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.	N/A	N/A	100GE and OTU4 OTU4 is supported only for the 200G-CK-LC card. Regeneration of any 100 G configuration 10GE 10GE 100GE

TXP-100G	100GS-CK-LC or 200G-CK-LC	N/A	N/A	N/A

Table 26: 100G-CK-C and 100ME-CKC Cards: Supported Configuration

Card Operating Modes	Trunk Card	Peer card	Skip Card	Supported Payload Types
TXP-100G	100G-CK-C/ 100ME-CKC	N/A	N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE
RGN-100G	100G-CK-C/ 100ME-CKC card and the peer card 100G-LC-C/ 100G-ME-C/ 100G-CK-C/ 100ME-CKC need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.		N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE
MXP-2x40G	100G-CK-C/ 100ME-CKC	N/A	N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE

Table 27: 100G-LC-C and 100G-ME-C Cards: Supported Configuration

Card Operating Modes	Trunk Card	Peer card	Skip Card	Supported Payload Types
TXP-100G	100G-LC-C/ 100G-ME-C	N/A	N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE
RGN-100G	100G-LC-C/ 100G-ME-C card and the peer card 100G-LC-C/ 100G-ME-C/ 100G-CK-C/ 100ME-CKC need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.		N/A	100GE, OTU4 — Regeneration of any 100 G configuration 40GE

Table 28: 10X10G-LC Cards: Supported Configuration

Card Operating Modes	Trunk Card	Peer card	Skip Card	Supported Payload Types
TXPP-10G	10x10G-LC	N/A	N/A	OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card. Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card. 10GE-LAN Phy, OTU2 10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G 10GE, 10G FC 10GE 10GE, OTU2e
TXP-10G	10x10G-LC	N/A	N/A	OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card. Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card. 10GE-LAN Phy, OTU2 10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G 10GE, 10G FC 10GE 10GE, OTU2e

MXP-10x10G	10x10G-LC card and the peer 100G-LC-C, 100G-ME-C, 100G-CK-C, 100ME-CKC, 100GS-CK-LC or 200G-CK-LC card need to be in adjacent slots 2-3, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15.	N/A	N/A	OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card. Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card. 10GE-LAN Phy, OTU2 10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G 10GE, 10G FC 10GE 10GE, OTU2e
RGN-10G	10x10G-LC	N/A	N/A	OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card. Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card. 10GE-LAN Phy, OTU2 10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G 10GE, 10G FC 10GE 10GE, OTU2e
LOW - LATENCY	10x10G-LC	N/A	N/A	N/A

FANOUT - 10X10G	10x10G-LC	N/A	N/A	OC192/STM-64, 10GE-LAN Phy, 10GE-WAN Phy (using OC192), OTU2, OTU2e, 8G FC, 10G FC, FICON Only OC192/STM64 and 10GE are supported when the 10x10G-LC card is connected with the 100GS-CK-LC card. Only OC192/STM64, 10GE, and OTU2 are supported when the 10x10G-LC card is connected with the 200G-CK-LC card. 10GE-LAN Phy, OTU2 10GE-LAN Phy, OTU2e, OTU2, OC192/STM-64, 8G FC, 10G FC, IB_5G 10GE, 10G FC 10GE 10GE, OTU2e

400G-XP-LC and MR-MXP cards of Cisco NCS 2000 devices can be configured with the following card operating mode and payload values:

- Payload types OTU2/OC192 are supported on MR-MXP cards,
- Payload types 16G-FC/OTU2 are supported on 400G-XP-LC cards,
- Slice operational mode OPM_6x16G_LC is supported on 400G-XP-LC cards.

Discover and Configure MPLS LDP and MPLS-TE Links

Using Cisco EPN Manager you can configure Label Distribution Protocol (LDP) and MPLS-TE links in an MPLS network.

MPLS LDP

LDP provides a standard methodology for hop-by-hop (or dynamic label) distribution in an MPLS network by assigning labels to routes that have been chosen by the underlying IGP routing protocols. The resulting labeled paths, called label switch paths (LSPs), forward labeled traffic across an MPLS backbone. Cisco EPN Manager enables you to configure the potential peers and establish LDP sessions with those peers to exchange information.

To configure LDP using Cisco EPN Manager you need to know the network address and interface of the device on which the LDP links must be configured and also subnet mask for the configured IP addresses.

Note Before configuring MPLS LDP, ensure that the LDP ID is pre-configured on the device.

MPLS-TE

Cisco EPN Manager supports the provisioning of MPLS Traffic Engineering (MPLS-TE) services. MPLS-TE enables an MPLS backbone to replicate and expand the TE capabilities of Layer 2 over Layer 3. MPLS TE

uses Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP) across the backbone. For more information, see, Supported MPLS Traffic Engineering Services, on page 495.

To configure LDP and MPLS-TE parameters:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Step 4 To configure LDP links:

a) Choose **MPLS > LDP**, click on **Common Properties** tab and and click '+' to specify new LDP parameters. To edit existing parameters, click the LDP Address hyperlink and click the Edit icon at the top right corner of the page.

Note You can only add a single set of LDP settings per device.

b) Under the **Common Properties** tab, specify the LDP parameters described in the below table.

MPLS LDP Fields	Field Descriptions
LDP Interface	Choose the LDP interface that is the source loopback interface for the LDP session on the device.
LDP Address	Specify the IP address of the LDP interface. Once the LDP address is set, it cannot be edited. To change the LDP address, delete the LDP session and create a new session with the new LDP address.
Session Hold Time	(Optional) Enter the time, in seconds, that the LDP session will go down if no hellos have been received after the Hold timer expires. Range is 15 to 65535.
NSR Enabled	Choose true or false to either enable or disable LDP nonstop routing (NSR). Enabling NSR allows the LDP to continue to operate across a node failure without losing peer sessions.
Discovery Hold time and Discovery Target Hold time	(Optional) Enter the time, in seconds, an LDP source and a discovered LDP neighbor is remembered without receipt of an LDP hello message from the neighbor. Range is 1 to 65535.
Discovery Hold Interval and Discovery Target Hold Interval	(Optional) Enter the time duration, in seconds, during which a LDP source and a discovered LDP neighbor is remembered. Range is 1 to 65535.
DownStream Min Label and DownStream Max Label	(Optional) Enter the minimum and maximum number of hops permitted in an LSP established by the Downstream on Demand method of label distribution. Range is 16 to 32767 for ISO XE and 16000 to 1048575 for ISO XR devices.
DownStream Max Hop Count	(Optional) Enter the number of hops permitted in an LSP established by the Downstream on Demand method of label distribution. Range is 1 to 255.
IGP Hold Down Time	(Optional) Enter the time, in seconds, to specify the time for which the declaration of LDP sync state is delayed after session establishment upon link coming up. Range is 1 to 2147483647 millisecond for ISO XE and 5 to 300 milliseconds for ISO XR devices.

MPLS LDP Fields	Field Descriptions
Entropy Enabled	Choose true or false to either enable or disable the MPLS LDP Entropy Label support feature which helps improve load balancing across MPLS networks using entropy labels.
Explicit Null Enabled	(Optional) Enable this value to advertise explicit-null labels for the directly connected route. Values are Yes (enabled) or No (disabled).
Initial Back Off and Max Back Off	(Optional) Enter the initial and maximum back off delay value in seconds. Range is 5 to 2147483.

c) Click **Save** to deploy your changes to the device.
d) Click on **Interfaces** tab and and click '+' to specify the Interface parameters.

MPLS LDP Fields	Field Descriptions
Interface Name	Specify the name of Interface to participate in the LDP session.
Label Distribution Method	Specify 'LDP' as the Label Distribution Method
Hello Interval	(Optional) Enter the time interval, in seconds, when hello messages will be sent. Range is 1 to 65535.

e) Click **Save** to deploy your changes to the device. The same properties are configured on the peer devices. Once the neighbor devices are formed, the details are populated in the **Neighbors** tab.

Step 5 To configure MPLS-TE links:

a) Choose **MPLS > MPLS-TE**. .
b) In the MPLS-TE FRR area, check the **MPLS TE Tunnel Enabled** check box. The default values of MPLS-TE parameters are displayed as described in the below table.

MPLS TE Tunnel Fields	Field Descriptions
MPLS TE Tunnel Enabled	Activates the display of the list of automatic bandwidth enabled tunnels, and indicates if the current signaled bandwidth of the tunnel is identical to the bandwidth that is applied by the automatic bandwidth
Auto Bandwidth Timer Frequency (Sec)	To set the interval (in seconds) at which the automatic bandwidth on a tunnel interface is triggered.
Reoptimize Timer Frequency (Sec)	Set the value (in seconds) to trigger the reoptimization interval of all TE tunnels.
Auto Backup Tunnel Enabled	To display information about automatically built MPLS-TE backup tunnels.
Backup Tunnel Min. Range and Backup Tunnel Max. Range	Configures the range of backup autotunnel numbers to be between the specified minimum and maximum value. Ensure that minimum range for the backup tunnel is lower than the maximum range.

MPLS TE Tunnel Fields	Field Descriptions
SRLG Exclude	Specifies an IP address to get SRLG values from, for exclusion. Choose one of the following options, if required: • Preferred • Forced • None **Note** SRLG Exclude option is available only for IOS-XE.
Un-numbered Interface	Enables IP processing on the specified interface without an explicit address.

Step 6 Click **Save** to deploy your changes to the device.

What to do next

Monitor LDP links on the Network Topology:

1. In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.
2. Click on the **Device Groups** button, select the required device group(s), and click **Load**.
3. Click **Show** in the topology toolbar and choose **Links**.
4. Select the **LDP** check box under Control Plane to display LDP links on the map.
5. Click on an LDP link to see details about the link.

For information on how to provision MPLS-TE services, see Provision MPLS Traffic Engineering Services, on page 582.

Analyze Ports Using SPAN and RSPAN

Using Cisco EPN Manager, you can analyze network traffic passing through ports or VLANs by using SPAN or RSPAN to send a copy of the traffic to another port on the switch or to a monitoring device. SPAN copies (or mirrors) traffic received or sent (or both) on source ports or source VLANs to a destination port for analysis. Traffic that enters or leaves source ports or traffic that enters or leaves source VLANs are monitored.

If you configure SPAN to monitor incoming traffic, then traffic that gets routed from another VLAN to the source VLAN cannot be monitored. However, traffic that is received on the source VLAN and routed to another VLAN can be monitored.

Cisco EPN Manager allows you to configure only one Local SPAN session per device. Local SPAN sessions copy traffic from one or more source ports in any VLAN to a destination port for analysis.

Using Remote SPAN you can configure source ports, source VLANs, and destination ports on different switches, enabling remote monitoring of multiple switches across your network. The traffic for each RSPAN session is carried over a user-specified RSPAN VLAN that is dedicated for that RSPAN session in all participating switches. The RSPAN traffic from the source ports or VLANs is copied into the RSPAN VLAN

and forwarded over trunk ports carrying the RSPAN VLAN to a destination session monitoring the RSPAN VLAN.

Note To monitor ports, you must ensure that the ports are associated with one or more VLANs (source or destination).

To enable port monitoring (or mirroring):

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device that you want to configure by clicking the device hyperlink to launch its Device Details page.

Step 3 Configure an RSPAN session:

a) Choose **Port Analyzer > RSPAN > Destination Node** to configure the destination node for RSPAN.

b) Click '+' to specify the RSPAN session ID. To edit existing settings, click the session ID hyperlink and click the Edit icon at the top right corner of the page.

You can add up to 14 RSPAN and SPAN sessions.

c) Choose a session ID and click **Save**.

The session type Remote Destination (Remote RSPAN) is set by default and cannot be edited.

d) Click the session ID hyperlink to specify the source and destination settings for the destination node.

e) Click the **Source Settings** tab, choose a valid VLAN ID (auto populated based on the VLANs configured on the selected device), and click **Save**.

You can add only a single VLAN as the source for the destination node. If no VLANs are configured, you need to configure them and return to this step. See View VLAN Interfaces, on page 354.

f) Click the **Destination Settings** tab, select the interface that must act as the destination node for the RSPAN, and click **Save**.

a) From the features panel, choose **Port Analyzer > RSPAN > Source Node** to configure the source node for RSPAN.

b) Click '+' to specify common RSPAN source node settings. To edit existing settings, click the session ID hyperlink and click the Edit icon at the top right corner of the page.

c) Choose a session ID and click **Save**.

The session type Remote Source (Remote SPAN) is set by default and cannot be edited.

d) Click the session ID hyperlink to specify the source and destination settings for the source node.

e) Click the **Source Settings** tab, specify the following values, and click **Save**.

i) In the **Interface** drop-down menu, choose the interface that will act as the source interface for the RSPAN source node.

An interface specified as a source node for RSPAN can also be used as the source/destination node for SPAN.

ii) In the **Direction** drop-down menu, choose direction in which the interface must be applied to the RSPAN source node. Your options are:

- **Transmit**: monitors all packets sent by the source interface after all modification and processing is performed by the switch. A copy of each packet sent by the source is sent to the destination port for that session. The copy is provided after the packet is modified.
- **Receive**: monitors all packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that session.

- **Both**: (default value) monitors a port or VLAN for both received and sent packets.

You can add multiple interfaces to the source node for RSPAN and then associate a single VLAN ID to these interfaces.

f) Click the **Destination Settings** tab, choose a valid VLAN ID (auto populated based on the VLANs configured on the selected device), and click **Save**.

Step 4 Configure a SPAN session:

a) Click **Port Analyzer > SPAN**.

b) Click the '+' to specify common SPAN source node settings. To edit existing settings, click the session ID hyperlink and click the Edit icon at the top right corner of the page.

Interfaces configured as the source and destination node for RSPAN, cannot be used for SPAN.

c) Choose a session ID and click **Save**.

The session type Local (Local SPAN) is set by default and cannot be edited.

d) Click the session ID hyperlink to specify the source and destination settings for SPAN.

e) Click the **Source Settings** tab, and choose the interface and direction in which the interface must be applied for SPAN, and click **Save**. For more details, see Step 4.

An interface specified as a source node for RSPAN can also be used as the source/destination node for SPAN.

f) Click the **Destination Settings** tab, choose a valid VLAN ID (auto populated based on the VLANs configured on the selected device), and click **Save**.

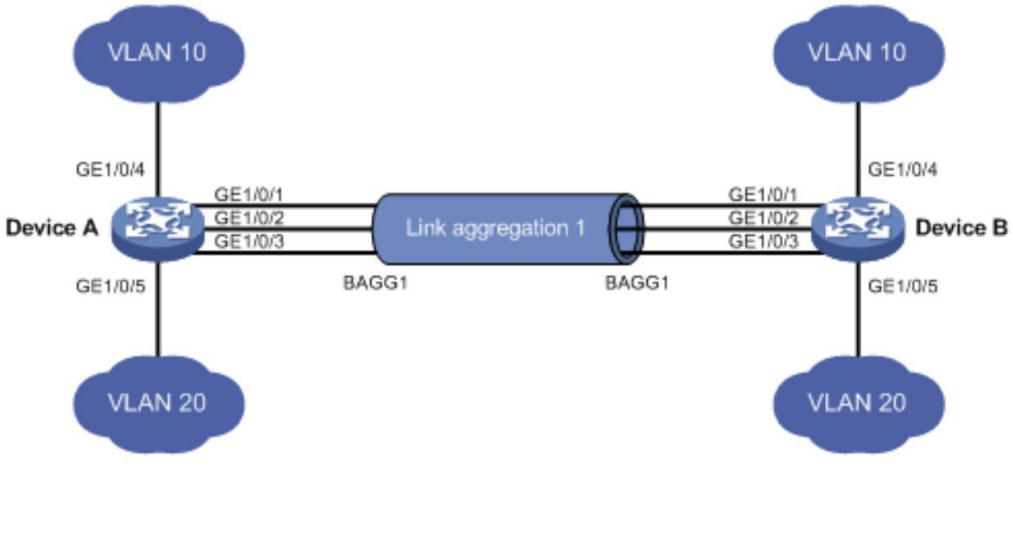
g) (Optional) To verify that your changes were configured correctly, use the following command in your device CLI:

```
show monitor session all
```

Configure and View Ethernet Link Aggregation Groups

An Ethernet Link Aggregation Group (LAG) is a group of one or more ports that are aggregated together and treated as a single link. Each bundle has a single MAC, a single IP address, and a single configuration set (such as ACLs). LAGs provide the ability to treat multiple switch ports as one switch port. The port groups act as a single logical port for high-bandwidth connections between two network elements. A single link aggregation group balances the traffic load across the links in the channel. LAGs help provision services with two links. If one of the links fails, traffic is moved to the other link.

The following figure illustrated a LAG created between two devices: Device A and Device B.



Cisco EPN Manager allows you to view and manage LAGs in the following ways:

- Create Link Aggregation Groups (LAG) Using Multiple Interfaces, on page 412
- View Ethernet LAG Properties, on page 413

Create Link Aggregation Groups (LAG) Using Multiple Interfaces

Using Cisco EPN Manager, you can create LAGs that provide the ability to treat multiple physical switch ports as a single logical one.

Before you begin

- Only interfaces that are not already part of an existing LAG can be selected. An interface cannot be part of more than one LAG.
- The selected group of interfaces must all consist of the same bandwidth type.
- Inventory collection status for the devices that participate in the LAG must be *Completed*.

To create a LAG:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Interfaces > Link Aggregation**.

Step 5 Depending on the type of control method that you want to use, click the **PAgP/MANUAL** or the **LACP** tab.

Step 6 To create a new LAG, click the Add (+) sign.

Step 7 Enter a unique name for the LAG. Ensure that the channel group ID that you specify is part of the LAG name. For example, for a channel group ID of 10, your LAG name should be:

- 'Bundle-Ether10' for Cisco IOS-XR devices.

Step 8 Enter a number between 1–16 to specify the Channel Group ID. The channel group ID ranges for different types of devices are: 1-8 for Cisco ASR 900 series devices, 1-64 for Cisco ASR 9200 series devices, 1-48 for Cisco NCS 4200 series devices, and 1-65535 for Cisco ASR 9000 series devices.

Step 9 Click the **Member Port Settings** tab to specify the member port values:

- LACP Modes: LACP can be configured with the following modes:
  - Active- In this mode, the ports send LACP packets at regular intervals to the partner ports.
  - Passive- In this mode, the ports do not send LACP packets until the partner port sends LACP packets. After receiving LACP packets from the partner port, the ports then send LACP packets to the partner port.
- PAgP Modes: PAgP modes can be configured with AUTO, DESIRABLE, or ON. For Cisco ASR 9000 devices, only On PAgP mode is enabled. ON implies that the mode is set to PAgP - manual.

Step 10 Click **Save**.

Your changes are saved and you can now add interfaces to the created LAG.

Step 11 To add interfaces to the created LAG, select the required channel group from the Link Aggregation table and click the Edit icon.

Step 12 Select the interfaces that you want to use to create the LAG.

Step 13 Click **Save**.

The LAG is created using the interfaces that you selected.

View Ethernet LAG Properties

To view the Ethernet LAG properties:

Procedure

	Command or Action	Purpose
Step 1	Go to **Configuration** > **Network Devices**.	
Step 2	Select the device on which you want to configure the LAG by clicking the device name hyperlink.	
Step 3	Click the **Device Details** tab.	
Step 4	Click **Interfaces > Link Aggregation** in the Features panel.	

Configure Routing Protocols and Security

Using Cisco EPN Manager, you can configure the following routing protocols for your CE and Optical devices. You can also configure security for your devices using ACLs.

Before you configure routing protocols and ACLs, ensure that the device's Inventory Collection status is 'Completed'.

To view a device's routing table, open the Device 360 view and choose **Actions** > **Routing Table Info** > **All**.

- Configure BGP, on page 414
- Configure an IS-IS, on page 417
- Configure OSPF, on page 419
- Configure Static Routing, on page 421
- Configure ACLs, on page 421

Configure BGP

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information between autonomous systems (AS) in your network. By configuring BGP, your device is enabled to make routing decisions based on paths, network policies, or rule-sets configured by a network administrator.

Using the Cisco EPN Manager, you can configure BGP routing and establish a BGP routing process by specifying the AS number and Router ID. You can then create a BGP neighbor which places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer. To configure the BGP neighbor, you need to provide the neighbor's IPv4 address and its peer AS number. BGP neighbors should be configured as part of BGP routing. To enable BGP routing, at least one neighbor and at least one address family must be preconfigured.

To view a device's BGP and BGP Neighbors routing table, open the Device 360 view, then choose **Actions** > **Routing Table Info**.

To configure BGP routing protocol on a device:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the required device by clicking the device name hyperlink.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Routing** > **BGP**.

Note The configuration changes on Cisco Catalyst 6500 Series devices with a quad-supervisor Virtual Switching System (VSS) are not dynamically reflected on this page. To view these changes, ensure that the 24 hour periodic device sync is completed. Alternatively, you can manually sync these devices with Cisco EPN Manager.

Step 5 To configure the BGP routing process, click the + icon or if BGP is already configured, click the AS number hyperlink and then click the Edit icon to enter the BGP Process details described in the table below.

Step 6 Click **Save** to deploy your changes to the device and to enable the BGP Address Family and BGP Neighbor tabs.

Step 7 To configure the BGP address family details, click the **BGP Address Family** tab and choose the address family details described in the table below, and click **Save**.

Step 8 To configure the BGP neighbor, click the **BGP Neighbor** tab and choose the neighbor device by selecting the device's IP address from the list.

Step 9 To create a new BGP neighbor, click the Add (+) icon, specify the following details described in the table below.

Step 10 Click **Save**. The updated BGP routing process values are saved and deployed to the selected device.

To verify that your changes were saved, go to **Configuration > Network Devices**, launch the Device Details page, and click the **Device Details**tab. Choose **Routing > BGP**. You can view your BGP configuration details such as the Neighbor Address, Remote AS, Address Family Type and Modifier, and Advertise Interval Time configured on the device.

Fields	Subfield	Descriptions
Common BGP Process fields	AS Number	Enter the AS number using a numeric value 1–4294967295.
	Router ID	• Enter the Router ID. The value can be an IPv4 address of the format: • A.B.C.D- for IPv4 addresses, where A, B, C, and D are integers ranging 0–255.
	Log Neighbor Changes	Select to track neighbor router changes.
BGP Address Family fields	BGP Global AF	• Address Family: Enter the BGP address family prefixes for the routing process. Your options are IPv4 and IPv6 (for unicast, multicast, and MVPN), VPNv4 and VPNv6 (for unicast), IPv4 (for MDT), and L2VPN_EVPN_AF (for EVPN-based services). • Allocate Label: Choose the labeled unicast address prefixes. • Allocate Label Custom Policy Name: Choose a custom policy to be associated with the routing process. **Note** The **Allocate Label** and **Allocate Label Custom Policy Name** fields are only applicable for IOS device types.
	BGP Additional Paths	Specify the details for the paths that enable the advertisement of multiple paths through the same peering session for the same prefix without the new paths implicitly replacing any previous paths. • Additional Paths: Choose whether the device must send, receive, or send and receive additional paths. This is done at the address family level or the neighbor level. During session establishment, the specified BGP neighbors negotiate the Additional Path capabilities (whether they can send and/or receive) between them. **Note** While configuring Cisco CAT65000 devices, you can configure only Install as the additional path value. • Best Value: This field is enabled only when the Additional Paths value that you choose supports the configuration of the Best Value field.
	BGP Neighbor AF	Specify the address family details that the specified BGP neighbor belongs to: • Neighbor Address: Choose the Router ID of the neighboring router. These values are populated based on the BGP neighbors created in the Neighbor tab. The value can be an IPv4 or an IPv6 address of the format:

Fields	Subfield	Descriptions
		• A.B.C.D- for IPv4 addresses, where A, B, C, and D are integers ranging 0–255. • xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx - for IPv6 addresses, where x would be a hexadecimal value and where the address uses eight sets of four hexadecimal addresses (16 bits in each set), separated by a colon (:). • Send Label: Choose the type of label that must be associated with the neighbor. • Route Reflector Client: Enable this field to configure the router as the route reflector and the specified neighbor as its client. • AIGP: Select to enable the accumulated interior gateway protocol (AIGP) path attribute. • Send Community: Choose how the community attributes must be sent to an external Border Gateway Protocol (eBGP) neighbor. • Next Hop Self: Select to set the BGP next-hop attribute of routes being advertised over a peering session to the local source address of the session. • Incoming and Outgoing Route Map Name: Choose to indicate whether a route policy must be applied to inbound or outbound updates from the neighbor.
	BGP Network Mask	• Network Address and Mask: Specify the network IP address and network mask for the specified IP address. • Back Door Route: Enable to set the administrative distance on an external Border Gateway Protocol (eBGP) route to that of a locally sourced BGP route, causing it to be less preferred than an Interior Gateway Protocol (IGP) route. • Network Route Policy Name: Choose the route policy that will be used to select prefixes for label allocation. This enables BGP to allocate labels for all or a filtered set of global routes (as dictated by the route policy).
BGP Neighbor tab fields	-	Specify the following values: • Peer AS Number- Enter the value for the autonomous system number using integers in the range 1–4294967295to. • Neighbor Address- Enter the IP address of the BGP neighbor that you want to configure. The value can be an IPv4 or an IPv6 address of the format. • A.B.C.D- for IPv4 addresses, where A, B, C, and D are integers ranging 0–255. • xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx - for IPv6 addresses, where x would be a hexadecimal value and where the address uses eight sets of four hexadecimal addresses (16 bits in each set), separated by a colon (:). • Local AS Number and Action: Specifies an autonomous-system number prepend to the AS_PATH attribute. The range of values is any valid autonomous system number 1–65535.

Fields	Subfield	Descriptions
		• Update Source: Use this option to establish a peer relationship (TCP connection) using the loopback interface as an alternative instead of using the interface closest to the peer router. • Fall-over: Select a value to enable the BGP fast peering session deactivation for improving the convergence and response time to adjacency changes with the specified BGP neighbor. • Password Encryption and Password: Specify whether password encryption is enabled or not, and if enabled, what the password value is. • (View only) Neighbor State: View the connection status of a neighbor device participating in a BGP routing process. The states are: Idle, Connect, Active, Open sent, Open confirm, and Established. The neighbor device generates events only when its connection status is Established. Check the connection status frequently in case there are updates from the device. **Note** The neighbor state value is not updated during a granular inventory sync. To see the updated values, wait for the sync to end successfully.

Configure an IS-IS

Intermediate System-to-Intermediate System (IS-IS) Protocol is an intra-domain OSI dynamic routing protocol which uses a two-level hierarchy to support large routing domains (administratively divided into areas). Routing within an area is referred to as Level 1 routing. Routing between areas is referred to as Level 2 routing. In order to enable IS-IS for IP on a Cisco router and have it exchange routing information with other IS-IS enabled routers, you must perform the following tasks:

- Enable the IS-IS routing process on the device and assign areas.
- Enable IS-IS IP routing on the required interfaces.

An interface with a valid IP address can be designated to act as a Level 1 (intra-area) router, a Level 1_2 (both a Level 1 router and a Level 2) router, or a Level 2 (an inter-area only) routing interface for a given IS-IS instance. After the IS-IS routing starts working across the routers between the designated interfaces, the IS-IS neighborhood is automatically generated.

Note To enable IS-IS routing, at least one address family must be configured by default. In this release, configuring address families cannot be done using Cisco EPN Manager.

To configure the IS-IS process on a device:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device on which you want to configure the IS-IS routing protocol by clicking the device name hyperlink.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Routing** > **ISIS**.

Step 5 To configure a new IS-IS process, click the '**+**' icon and enter the following parameters:

- Specify the **IS-IS Process ID** using alphanumeric characters only. No spaces or special characters are allowed.
- Specify the **NET ID** in NSAP format. For example, your NET ID can be 49.0001.0000.0001.0010.00, where:
  - 49 - represents the first portion of the area ID which represents the AFI (Authority and Format Indicator).
  - 0001 - represents the second portion of the area ID.
  - 0000.0001.0010 - represents the system ID.
  - 00 - represents the N-selector which is always 0.
- Specify the type of IS-IS routing protocol in the **IS-IS Type** field. Your options are: Level 1, Level 2, and Level 1_2.

Step 6 Click **Save**.

Step 7 To configure this routing process on the selected device's interfaces:

a) Select the IS-IS protocol process created in the above steps from the **Routing** > **IS-IS** list.
b) Click the IS-IS process ID hyperlink.
c) Use the **IS-IS Interfaces** tab to specify the interfaces of the device on which the selected IS-IS configuration is to be applied:
   - Click the '**+**' icon to enter the interface details.
   - From the **Circuit Type** drop-down menu, select the type of circuit to which this configuration is to be applied. Your options are: Level 1, Level 2, and Level 1_2.
   - From the **Interface** drop-down menu, select the required interfaces.
   - (Optional) Specify the Level 1 and Level 2 metric and priority values. For the **Priority** field enter a value between 1 to 127 and for the **Metric**, a value between 1 to 16777214.
   - Enable the **Point-to-Point** checkbox to enable point to point connection.
   - Click **Save** to deploy the configuration onto the selected interfaces.

Step 8 Click **Save**. The selected IS-IS process is configured on the specified interfaces of the device.

Step 9 (Optional) To view IS-IS neighbors associated with the selected device, click the IS-IS hyperlink and click the **IS-IS Neighbors** tab. You can view the configured neighbor's hostnames, IP addresses, system IDs, IS-IS types, their connection states, the configured hold down time values, and the local interface names.

Note If the hostnames of the IS-IS neighbors are greater than 15 unique characters, the hostnames are not displayed in Cisco EPN Manager. Ensure that the hostnames are not more than 15 unique characters.

Step 10 (Optional) To delete IS-IS routing processes configured using Cisco EPN Manager:

a) Go to **Configuration > Network Devices**, launch the Device Details page, and choose **Routing > IS-IS**.
b) Select the required IS-IS process from the list.
c) Click the '**x**' icon to delete and click **OK** to confirm the delete operation.

Configure OSPF

Open Shortest Path First (OSPF) is a standards-based routing protocol that uses the Shortest Path First (SPF) algorithm to determine the best route to its destination. OSPF sends Link State Advertisements (LSAs) to all routers within the same configured area. OSPF sends routing updates only for the changes in the routing table; it does not send the entire routing table at regular intervals.

Using Cisco EPN Manager you can configure OSPF for IPv4 and IPv6 addresses. To do this, ensure that you know the router ID, the administrative distance that you want to configure on the router, and the maximum path values to be set.

To configure the OSPF routing process:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device on which you want to enable OSPF by clicking the device name hyperlink. Select only IOS-XR devices.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Routing > OSPF** .

Note The configuration changes on Cisco Catalyst 6500 Series devices with a quad-supervisor Virtual Switching System (VSS) are not dynamically reflected on this page. To view these changes, ensure that the 24 hour periodic device sync is completed. Alternatively, you can manually sync these devices with Cisco EPN Manager.

Step 5 To add a new OSPF process, click the + sign. To modify existing OSPF processes, select the required process by clicking the process ID hyperlink and click the Edit icon at the top right corner of the page.

Step 6 Specify the common OSPF parameters as described in the table below.

Step 7 Click **Save**. Your configuration changes are saved. To verify, click the **Configuration** tab, choose **Routing** > **OSPF**, and view the displayed details.

Step 8 Specify the **OSPF Interfaces** settings:

Once you have configured the OSPF process with basic properties, you can further deploy that configuration directly on an entire network or on an OSPF area. To do this, you need to specify the OSPF area ID, the device's interface details, the network type, etc. To change OSPF interface settings:

a) Choose **Configuration** > **Network Devices**.
b) Select the device on which you want to configure these changes by clicking the device name hyperlink.
c) Click the **Configuration** tab and choose **Routing > OSPF** .
d) Select the required process by clicking the process ID hyperlink.
e) Click the **OSPF Interfaces** tab.
f) Click the Add ('+') icon to add new settings to the interfaces associated with the selected device's OSPF process. To edit existing values, click the Interface Name hyperlink and click the Edit icon at the top right of the page.
g) Specify the parameters as explained in the table below.
h) Click **Save** to deploy your changes to the device.

Option	Description
OSPF Common Properties	**Description**
Process ID	Unique numerical value between 1 and 65535 that identifies the selected OSPF process.
Router ID	Router ID of the Area 0 router.

Option	Description
Cost	Sets a cost for sending packets across the network, which is used by OSPF routers to calculate the shortest path. This is not enabled for Cisco IOS-XE devices. Enter a numeric value between 1 and 65535.
Topology Priority	Displays the designated router for a subnet. Enter a numeric value between 1 and 255.
Maximum number of paths per route	Defines the highest number of paths that can be used by the router for load balancing per route. The default value is 4. You can set a numeric value between 1 and 64.
Administrative Distance	Specifies the distance that will be set for path selection. The default value is 110 and the available values are between 1 and 255.
External Area Distance	Specify the distance for external type 5 and type 7 routes. Your options are any numeric value between 1 and 255.
Inter Area Distance	Specify the inter area distance for inter-area routes using a value between 1 and 255.
Intra Area Distance	Specify the intra area distance for intra-area routes using a value between 1 and 255.
Routing > OSPF > OSPF Interface/PEP Properties	**Description**
Area ID	Specify the OSPF area ID for the NEs using an integer between the 0 and 4294967295. The ID cannot be 0.0.0.0.
Interface Name	Device's interface with which the specified OSPF interface/pep settings must be associated.
Interface cost	Cost of sending packets across the network. This cost is used by OSPF routers to calculate the shortest path.
Interface Priority	Designated router for a subnet.
Network Type	Type of network associated with the OSPF process. Your options are: Broadcast, NBMA, Point to Point, and Point to Multipoint.
Dead Interval	Number of seconds that will pass while an OSPF router's packets are not visible before its neighbors declare the router down. The Cisco default is 40 seconds.
Hello Interval	Number of seconds between OSPF hello packet advertisements sent by OSPF routers. The Cisco default is 10 seconds.
Retransmit Interval	Time that will elapse before a packet is resent. The Cisco default is 5 seconds.
Transmit Delay	Service speed. The Cisco default is 1 second.

Configure Static Routing

Static routing is the simplest form of routing, where the network administrator manually enters routes into a routing table. The route does not change until the network administrator changes it. Static routing is normally used when there are very few devices to be configured and the administrator is very sure that the routes do not change. The main drawback of static routing is that a change in the network topology or a failure in the external network cannot be handled, because routes that are configured manually must be updated to fix any lost connectivity.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Routing** > **Static**.

Step 5 To configure static routing, click **Add**.

a) If you are adding an IPv4 static route, in the IPv4 Static Routes area, click the Add (+) icon. Enter the required details in the following fields:

Destination Network, Network Mask, Next Hop IP, Outgoing Interface, Permanent Route, or Administrative Distance.

b) If you are adding an IPv6 static route, in the IPv6 Static Routes area, click the Add (+) icon. Enter the required details in the following fields:

Destination IPv6 Prefix, Prefix Length, Next Hop IPv6 Address, Outgoing interface, Administrative Distance, Cast Type, or Tag Value.

Step 6 Click **Save**.

Configure ACLs

The Configuration tab in the Device Details page lists the current CFM configuration on the device. Depending on your device configuration and user account privileges, you can configure ACLs on the device.

To configure ACLs:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Click the device hyperlink to launch its Device Details page.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Security** > **ACL**.

Step 5 Specify the following parameters for the ACL:

a) Name/Number- Specify a unique identifier for the ACL. You can use alphanumeric characters, hyphens, and underscores.

b) Type- Specify whether the ACL is of type standard or extended. This drop-down menu is hidden depending on the type of device you select. For example, for Cisco IOS-XR devices this drop-down menu is hidden.

c) (Optional) Description- Enter a description about the ACL for reference.

Step 6 Click **Save** to save your values in the Cisco EPN Manager. This does not deploy your changes to the device.

Step 7 Click the drop-down icon next to the ACL created in the above steps and specify the following ACE values:

a) Click **Add Row** to add a new ACE or select an existing ACE and click **Edit**, to specify the Action (Permit or Deny), Source IP, Destination IP and optionally the wild card source, port information and description that must be associated with the ACE.

b) Click **Save** to save the values associated with the ACE.

c) Use the up and down arrows (buttons) to specify the order in which the ACEs must be applied on the device for the selected ACL.

Step 8 Select the ACL created in the above steps and click **Apply to Interface** to specify the interface(s) on which this ACL must be applied.

Step 9 Click **OK** to deploy the specified ACL values to the selected interfaces of the device.

Configure Segment Routing

Segment routing (SR) uses the concept of source routing, where the source chooses a path, either explicit or Interior Gateway Protocol (IGP) shortest path and encodes the path in the packet header as an ordered list of segments. Segments are sub-paths that a router can combine to form a complete route to a network destination. Each segment is identified by a segment identifier (SID) that is distributed throughout the network, using new IGP extensions.

From the Cisco EPN Manager GUI, you can leverage the following Segment Routing sub-menu options to configure Segment Routing parameters on your devices. You can also view or edit Segment Routing settings that have been configured from the CLI.

- Configure Segment Settings
- Configure Routing Process
- Configure PCE Server
- Configure Path Computation Client (PCC)
- Configure Affinity
- Configure On-Demand Policy

The following table lists the devices for which Segment Routing parameters can be configured from the UI, along with their supported software versions.

Device Series & Types	Software Versions
NCS 540	6.5.3, 6.6.1, 7.0.1, 7.1.1
NCS 560	6.5.3, 6.6.1, 7.0.1, 7.1.1
NCS 5500	6.5.3, 6.6.1, 7.0.1, 7.1.1
ASR 9000	6.5.3, 6.6.1, 7.0.1, 7.1.1

Configure Segment Settings

To configure the global settings for Segment Routing for the selected device:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device for which you want to configure the segment routing settings by clicking the device name hyperlink.

Step 3 Click the **Device Details** from the tab on the left.

Step 4 Choose **Segment Routing** > **Segment Settings**.

Step 5 Under the **General tab**, click '**+**' to enter the required values and click **Save**. To edit an existing configuration, click the corresponding hyperlink.

Attributes	Description
Global Block Min	The Segment Routing Global Block (SRGB) is a range of label values preserved for segment routing in the label switching database. The SRGB label values are assigned as prefix segment identifiers (SIDs) to SR-enabled nodes and are valid across the domain. Enter a value between 16000 and 1048575.
Global Block Max	
Local Block Min	The Segment Routing Local Block (SRLB) is a range of label values preserved for the manual allocation of adjacency segment identifiers (adj-SIDs). These labels are locally significant and are only valid on the nodes that allocate the labels. Enter a value between 15000 and 1048575.
Local Block Max	
Binding SID	Select a value from the drop-down list.
Maximum SID Depth	The number of SIDs supported by a node or by a link on a node. Enter a value between 1 and 255.

Note Run the following command to clear the label discrepancy for SRGB or SRLB changes to take effect.

```
#clear segment-routing local-block discrepancy all
```

Step 6 Under the **Mapping Server** tab, click '**+**' to enter the required values and click **Save**. Click **Ok** to confirm that you want to push your changes to the device. To delete an existing configuration, select the corresponding checkbox and click '**X**'.

Attribute	Description
IP Address Prefix	Enter an IPv4 address.
Mask	Enter the subnet mask details.
Address Family	Choose the address family as IPv4.
Start of SID Range	Enter a value between 0 and 1048575.
Number of Allocated SIDs	Enter a value between 0 and 1048575. The default value is 1.

Step 7 Under the **Adjacency SID Mapping** tab, click '**+**' to enter the required values and click **Save**. Click **Ok** to confirm that you want to push your changes to the device. To delete an existing configuration, select the corresponding checkbox and click '**X**'.

Attribute	Description
Interface	Select a loopback interface from the dropdown list.
Address Family	Choose the address family as IPv4.
Next Hop Address	Enter an IPv4 address for the next hop.
SID Mapping Type	Select either Absolute or Index as the mapping type.
SID Value	The valid range for the SID value varies according to the SID mapping type. • For Index type – 0 to 1048575 • For Absolute type – 15000 to 1048575

Configure Routing Process

To configure Routing Process parameters for Segment Routing for the selected device:

Before you begin

Before configuring Routing Process parameters, ensure that you have configured OSPF or ISIS routing process on the device from **Device Details** > **Routing** page. See Configure Routing Protocols and Security, on page 413 for more information.

Note Cisco EPN Manger does not support OSPFV3 protocol in Segment Routing.

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device for which you want to configure the parameters by clicking the device name hyperlink.

Step 3 Click the **Device Details** from the tab on the left.

Step 4 Click **Segment Routing** > **Routing Process**.

Step 5 Enter values for the attributes as necessary under each tab by clicking the corresponding hyperlink and click **Save**.

Tab	Attributes	Description
Properties	Process ID	This field is populated automatically with the process ID configured on the device.
	Process Type	This field is populated automatically as ISIS or OSPF based on the configuration on the device.
	Global Block Min	The default SRGB range is from 16000 to 23999. The values entered here will override the global values configured in **Segment Settings**.
	Global Block Max	
	Advertise Local Prefix SID Mapping	By default, this field is enabled
	Override LDP Labels	Select this check box to override LDP labels.
	Receive Remote Prefix SID Mapping	Select this check box to receive Remote Prefix SID Mapping
	Avoid Microloop	Select this check box to avoid microloop.
Connected Prefix SID Mapping	Ip Address Prefix	Enter an IPv4 address
	Mask	Enter subnet mask details
	SID Mapping Type	Select either Absolute or Index mapping type from the drop-down list.
	SID Value	The valid range for the SID value varies according to the SID mapping type. • For Index type – 0 to 1048575 • For Absolute type – 16000 to 1048575
	Flex Algorithm	Enter Flex Algorithm value between 128 and 255. This field is grayed out if Strict SPF is enabled.
	Strict SPF	Select the check box if required
	Replace Prefix SID with Explicit Null	Select the check box if required

Tab	Attributes	Description
Interface Prefix SID Mapping	SID Mapping Type	Select either Absolute or Index mapping type from the drop-down list.
	SID Value	The valid range for the SID value varies according to the SID mapping type. • For Index type – 0 to 1048575 • For Absolute type – 16000 to 1048575
	Strict SPF	Select the check box if required
	Replace Prefix SID with Explicit Null	Select the check box if required

Note

- For ISIS routing process, you can configure either connected prefix or local prefix. For OSPF Routing process, only local prefix SID configuration is supported.
- For configuring local prefix SID, only loop back interfaces where IP is configured will be modeled under Routing Process.
- For local prefix SID, the device supports the following configuration:
  - prefix-sid index/absolute 100 explicit-null (prefix-sid without algorithm/strict-spf)
  - prefix-sid algorithm 128 index /absolute 16000 (prefix-sid with algorithm)
  - prefix-sid strict-spf index/absolute 200 explicit-null (prefix-sid with strict-spf)

Configure Path Computation Client (PCC)

To configure PCC client parameters for the selected device:

Before you begin

- PCC is a one-time configuration that must be discovered in advance in order to be presented and modified in EPNM.

  Sample configuration:

  ```
  segment-routing
  traffic-eng
  pcc
  ```

- To receive PCC-peer events, the device should be enabled with pcep peer-status logging under segment-routing traffic-eng logging.

Step 1 Choose **Configuration** > **Network Devices**.

Step 2 Select the device for which you want to configure the parameters by clicking the device name hyperlink.

Step 3 Click the **Device Details** from the tab on the left.

Step 4 Click **Segment Routing** > **PCC**.

Step 5 Enter values for the attributes as necessary under each tab by clicking the corresponding hyperlink and click **Save**. Confirm that you want to push your changes to the device by clicking **Ok**.

Tab	Attribute	Description
PCC	Source Address	Enter an IPv4 address.
	Report All	Select the check box to set this value to True.
	PCC Centric Model	Select the check box to set this value to True.
	Session Dead time	Measured in seconds. Enter a value 0–255.
	Session Keepalive Time	Measured in seconds. Enter a value 0–255. Enter 0 if you wish to disable this parameter.
	Delegated Policy Up Timeout	Measured in seconds. Enter a value 0–3600. Enter 0 if you wish to disable this parameter.
	PCE Initiated Orphan State Time	Enter a value 15–14400.
	PCE Initiated Policy Delegation Time	Enter a value 10–180 seconds.
PCC's Peer Database	PCE Address	Enter an IPv4 address.
	Precedence	Enter a number 0–255 to set precedence. 0 is the most preferred and 255 is the least preferred..
	Password	Enter password (clear text password) and keychain details for client-server authentication.
	Keychain	

Configure PCE Server

To configure the selected device as a PCE server:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device for which you want to configure the parameters by clicking the device name hyperlink.

Step 3 Click the **Device Details** from the tab on the left.

Step 4 Click **Segment Routing** > **PCE Server**.

Step 5 Click the '+' to enter required values and click **Save**. Confirm that you want to push your changes to the device by clicking **Ok**.

Tab	Attribute	Description
PCE Server	IP Address	Enter an IPv4 address.
	State Sync Address	Enter multiple IPv4 addresses separated by a comma.
	Keepalive Time	Measured in seconds. Enter a value between 0–255. The default value is 30. Enter 0 to disable this parameter.
	Password	Enter password (clear text) to authenticate client-sever details.
	Minimum Peer Keepalive Interval	Measured in seconds. Enter a numeric value between 0–255. The default value is 20. Enter 0 to disable this parameter.
	Strict SIDs Only	Select the check box to enable this option. This option is not enabled by default.
	Topology Reoptimization Interval	Measured in seconds. Enter a value between 600–86400. The default value is 1800.

Note Due to device and network limitations, you cannot delete a PCE Server once you've configured it.

Configure Affinity

To configure Affinity parameters for Segment Routing for the selected device:

Step 1 Choose **Configuration** > **Network Devices**.

Step 2 Select the device for which you want to configure the parameters by clicking the device name hyperlink.

Step 3 Click the **Device Details** tab.

Step 4 Choose **Segment Routing** > **Affinity**.

Step 5 Click the '**+**' icon to enter the required values and click **Save**. Click OK to confirm that you want to push your changes to the device. To edit, click the corresponding hyperlink. To delete an existing configuration, select the corresponding checkbox and click '**X**'.

Tab	Attribute	Description
Affinity	Affinity Name	Enter a name for the Affinity attribute.
	Bit Position	Enter a value 0–255.
Affinity Mapping	Interface Name	Select a loopback interface from the dropdown list to associate an interface to the Affinity. You must associate at least one Affinity with an interface.
	Affinity Name	Select the Affinity to be associated with the interface from the drop-down list. You can associate multiple affinities to a single interface.
	Metric value	Enter a value 0–2147485647

Configure On-Demand Policy

To configure On-Demand policy parameters for Segment Routing for the selected device, complete the following steps:

Step 1 Choose **Configuration** > **Network** > **Network Devices**.

Step 2 Select the device for which you want to configure the parameters by clicking the device name hyperlink.

Step 3 Click the **Device Details** from the tab on the left.

Step 4 Click **Segment Routing** > **On-Demand Policy**.

Step 5 Click the '**+**' icon to enter the required values and click **Save**. Click OK to confirm that you want to push your changes to the device. To edit, click the corresponding hyperlink. To delete an existing configuration, select the corresponding check box and click 'X'.

Tab	Attribute	Description
On-Demand Policy Template	Color	Enter a value 1–4294901295.
	Bandwidth	Enter a value 1–4294967295 in kbps.
	Path type	Select a value from the drop-down list.
	Max SID Limit	Enter a value 1–255.
	Metric Margin Mode	Select a value from the drop-down list.
	Metric Type	Select a metric type from the drop-down list.
	Metric Margin Value	Enter a value 0–2147483647.
Flex Algorithm	Color	This field is automatically populated with the value entered in On-Demand Policy Template tab.
	Flex Algorithm	Enter Prefix-SID algorithm value 128–255.
Disjoint Path	Color	This field is automatically populated with the value entered in On-Demand Policy Template tab.
	Group Id	Enter a value 1–65535.
	Disjointness Type	Use the drop-down list to choose a value.
	Sub Group Id	Enter a value 1–65535.

To configure Segment Routing policies, see Create and Provision Segment Routing Policies, on page 522.

Configure EOAM Fault and Performance Monitoring

Cisco EPN Manager enables you to prepare the devices in your network for using EOAM (Ethernet Operations, Administration and Management) protocol for monitoring and troubleshooting Carrier Ethernet services. You can perform connectivity and performance tests on the Ethernet services using sets of CLI commands available as predefined templates in Cisco EPN Manager.

Configure CFM

CFM configuration sets the stage for using the EOAM protocol to monitor and troubleshoot Carrier Ethernet services. CFM can be configured on the EVC level when creating and provisioning an EVC, as described in Create and Provision a New Carrier Ethernet EVC, on page 508.

Once CFM is configured, you can quickly and easily view the CFM settings on individual devices.

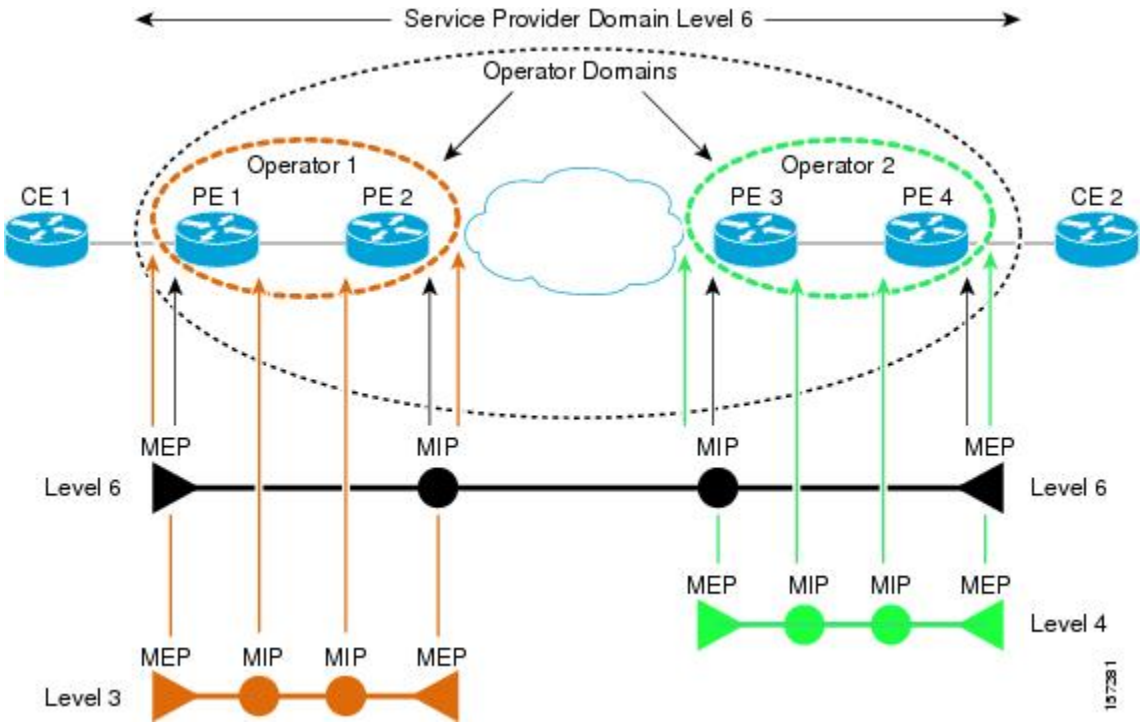
CFM Overview

IEEE Connectivity Fault Management (CFM) is an end-to-end per-service Ethernet layer Operations, Administration, and Maintenance (OAM) protocol. CFM includes proactive connectivity monitoring, fault verification, and fault isolation for large Ethernet metropolitan-area networks (MANs) and WANs.

CFM operates on a per-Service-VLAN (or per-EVC) basis. It lets you know if an EVC has failed, and if so, provides the tools to rapidly isolate the failure.

A CFM-enabled network is made up of maintenance domains, CFM services and maintenance points, as described below.

Figure 11: CFM Maintenance Domains



Maintenance Domains

Ethernet CFM, within any given service provider network, relies on a functional model consisting of hierarchical maintenance domains. A maintenance domain is a management space on a network that is owned and operated by a single entity and defined by a set of internal boundary ports. A domain is assigned a unique maintenance level which defines the hierarchical relationship of domains. Maintenance domains may nest or touch, but cannot intersect. If two domains nest, the outer domain must have a higher maintenance level than the one it engulfs. A single device might participate in multiple maintenance domains.

CFM Services

A CFM service (maintenance association) enables the partitioning of a CFM maintenance domain according to the connectivity within the network. For example, if the network is divided into a number of virtual LANs (VLANs), a CFM service is created for each of these. CFM can then operate independently in each service.

A CFM service is always associated with the maintenance domain within which it operates, and therefore with that domain's maintenance level. All CFM frames relating to the service carry the maintenance level of the associated maintenance domain. There can be many CFM services within a domain. The CFM service must be configured on a domain before MEPs can be configured.

Maintenance Points

A maintenance point demarcates an interface that participates in a CFM maintenance domain. A maintenance point is an instance of a particular CFM service on a specific interface. CFM only operates on an interface if there is a CFM maintenance point on the interface. A maintenance point is always associated with a particular CFM service, and therefore with a particular maintenance domain at a particular level. Maintenance points generally only process CFM frames at the same level as their associated maintenance domain. Frames at a higher maintenance level are always forwarded transparently, while frames at a lower maintenance level are normally dropped. This helps enforce the maintenance domain hierarchy and ensures that CFM frames for a particular domain cannot leak out beyond the boundary of the domain. There are two types of maintenance points:

- Maintenance endpoints (MEPs)—Created at the edge of the domain. Responsible for confining CFM messages within the domain. Maintenance end points (MEPs) are members of a particular service within a domain and are responsible for sourcing and sinking CFM frames. They periodically transmit continuity check messages and receive similar messages from other MEPs within their domain. They also transmit traceroute and loopback messages at the request of the administrator.
- Maintenance intermediate points (MIPs)—Internal to the domain. A MIP will forward CFM packets while MEPs do not forward CFM packets because they must keep them within the domain. MIPs are not explicitly configured on each interface. MIPs are created automatically according to the algorithm specified in the CFM 802.1ag standard.

View CFM Maintenance Domains and Maintenance Associations (Services)

To view CFM settings on a device:

Step 1 Choose **Configuration** > **Network** > **Network Devices**from the left sidebar.

Step 2 Locate the required device in the list of devices and click the device name hyperlink to open the device details window.

Step 3 Click the **Device Details** tab.

Step 4 Choose **EOAM > CFM**.

Perform EOAM Connectivity and Performance Checks

Cisco EPN Manager provides predefined EOAM-related configuration templates that can be used to monitor the connectivity and performance of virtual connections (VCs) in a Carrier Ethernet network.

To use these templates, from the left sidebar, choose **Configuration** > **Templates** > **Features & Technologies**, then choose **CLI Templates** > **System Templates – CLI**.

The following table lists the available EOAM configuration templates, their purpose, and the mandatory input parameters you are required to provide.

Note To see the results and/or output of template deployment, check the job details that are displayed when you deploy a change.

Table 29: EOAM Templates

Template Name	Use it to...	Essential Input Values	Additional Information
EOAM-CCDB-Content-IOS	Display the contents of a maintenance intermediate point (MIP) continuity check database (CCDB) in order to verify CFM operation or to check how EOAM has been set up in the network.	None of the fields are mandatory. **Domain ID:** Choose the way in which you want to identify the maintenance domain and enter a value in the corresponding field. **Service:** Specify a maintenance association within the domain, based on ICC MEG identifier, VLAN ID or VPN ID.	
EOAM-CCDB-Content-IOS-XR	Display the contents of a maintenance intermediate point (MIP) continuity check database (CCDB) in order to verify CFM operation or to check how EOAM has been set up in the network.	None of the fields are mandatory. **Node ID:** The CFM CCM learning database for the designated node, entered in the rack/slot/module notation.	
EOAM-CFM-Ping-IOS and EOAM-CFM-Ping-IOS-XR	Check connectivity to a destination MIP or MEP using CFM loopback messages.	**Ping Destination Type:** Identify the destination MEP, either by MAC address or MEP ID. Choose Multicast if there are multiple destination MEPs. Maintenance domain name for destination MEP: The name of the domain where the destination MEP resides.	
EOAM-CFM-Traceroute-IOS	IOS devices: Trace the route to a destination MEP to check the number of hops and the connectivity between hops.	**Destination Type:** Identify the destination MEP, by MAC address, MEP ID or explore options. **Maintenance domain name for destination MEP:** The name of the domain where the destination MEP resides. **Service Type:** Identify the maintenance association (MA) within the domain, either by name, ITU carrier code (ICC), MA number, VLAN ID, or VPN ID.	

Template Name	Use it to...	Essential Input Values	Additional Information
EOAM-CFM-Traceroute-IOS-XR	IOS-XR devices: Trace the route to a destination MEP to check the number of hops and the connectivity between hops.	**Maintenance domain name for destination MEP:** The name of the domain where the destination MEP resides. **Service Name:** The name of the service instance being monitored by the Maintenance Association (MA) within the specified maintenance domain. **Destination Type:** Identify the destination MEP, either by MAC address, MEP ID or explore options. **Source MEP ID:** Identify the maintenance association (MA) within the domain, either by name, ITU carrier code (ICC), MA number, VLAN ID, or VPN ID. **Source Interface Type:** The source interface type of the locally defined CFM MEP. **Interface Path ID:** The physical or virtual interface name.	
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Loopback-IOS-XR	Configure an on-demand Ethernet SLA operation for CFM loopback. By default, measures two-way delay and jitter.	**Probe Domain:** Check the checkbox to enable the probe. **Domain Name:** The name of the maintenance domain for the locally defined CFM MEP. **Domain Interface Type:** The source interface type of the locally defined CFM MEP. **Domain Interface Path ID:** The physical or virtual interface name. **Domain MAC Address or MEP-ID:** Choose whether you want to identify the domain by MAC address or by MEP ID and provide the necessary information in the relevant field below. For MEP ID, enter an ID from 1 to 8191.	Optionally, you can specify the type of statistics to measure, whether or not to use bins for aggregate type, probe frequency and duration values, and more. The values you specify will override the default actions.

Template Name	Use it to...	Essential Input Values	Additional Information
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Synthetic-Loss-Measurement-IOS-XR	Configure an on-demand Ethernet SLA operation for CFM synthetic loss measurement. By default, measures one-way Frame Loss Ratio (FLR) in both directions.	**Probe Domain:** Check the checkbox to enable the probe. **Domain Name:** The name of the maintenance domain for the locally defined CFM MEP. **Domain Interface Type:** The source interface type of the locally defined CFM MEP. **Domain Interface Path ID:** The physical or virtual interface name. **Domain MAC Address or MEP-ID:** Choose whether you want to identify the domain by MAC address or by MEP ID and provide the necessary information in the relevant field below. For MEP ID, enter an ID from 1 to 8191.	Optionally, you can specify the type of statistics to measure, whether or not to use bins for aggregate type, probe frequency and duration values, and more. The values you specify will override the default actions.
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Delay-Measurement-IOS-XR	Configure an on-demand Ethernet SLA operation for CFM delay measurement. By default, measures one-way delay and jitter in both directions, and two-way delay and jitter.	**Probe Domain:** Check the checkbox to enable the probe. **Domain Name:** The name of the maintenance domain for the locally defined CFM MEP. **Domain Interface Type:** The source interface type of the locally defined CFM MEP. **Domain Interface Path ID:** The physical or virtual interface name. **Domain MAC Address or MEP-ID:** Choose whether you want to identify the domain by MAC address or by MEP ID and provide the necessary information in the relevant field below. For MEP ID, enter an ID from 1 to 8191.	Optionally, you can specify the type of statistics to measure, whether or not to use bins for aggregate type, probe frequency and duration values, and more. The values you specify will override the default actions.

Template Name	Use it to...	Essential Input Values	Additional Information
EOAM-Configure-Y-1731-PM-Direct-On-Demand-IOS	Perform real-time troubleshooting of Ethernet services in direct mode where an operation is created and run immediately.	Frame Type: The type of frame, either DMMv1 (frame delay) or SLM (frame loss). Domain Name: The name of the maintenance domain for the locally defined CFM MEP. EVC or VLAN: Identify the EVC or VLAN on which the test will be performed. The VLAN ID can be between 1 and 4096. Target MPID or MAC Address: Identify the MEP at the destination, either by MPID (1 to 8191) or by MAC Address. CoS Value: The class of service level (0-7) that will be applied to the CFM message for the specified MEP. Local MPID or MAC Address: Identify the MEP at the source, either by MPID (1 to 8191) or by MAC Address. Burst or Continuous: Specify whether a continuous stream of frames or bursts of frames will be sent during the on-demand operation. Aggregation Period: Specify the length of time in seconds during which the performance measurements are conducted, after which the statistics are generated (1-900).	
EOAM-Configure-Y-1731-PM-Referenced-On-Demand-IOS	Perform real-time troubleshooting of Ethernet services in referenced mode where a previously configured operation is started and run.	Frame Type: The type of probe, either DMMv1 or SLM. Operation Number: The number of the operation being referenced.	
Remove-CFM-MEP- IOS	Remove the MEP configuration from the device.	Interface Name, Service Instance Number,EVC Name.	
Remove-CFM-MEP-IOSXR	Remove the MEP configuration from the device.	Interface Name, Domain Name.	
Remove-CFM-Service-IOS	Remove the CFM service.	Interface Name, Service Instance Number, EVC Name, Domain Name, Level, Service Name.	

Configure Quality of Service (QoS)

Quality of Service (QoS) is a set of capabilities that allow the delivery of differentiated services for the network traffic. QoS features provide better and more predictable network service by:

- Giving preferential treatment to different classes of network traffic.
- Supporting dedicated bandwidth for critical users and applications.
- Controlling jitter and latency (required by real-time traffic).
- Avoiding and managing network congestion.
- Shaping network traffic to smooth the traffic flow.
- Setting traffic priorities across the network.

Using Cisco EPN Manager you can configure QoS on Carrier Ethernet interfaces. Before the appropriate QoS actions can be applied, the relevant traffic must be differentiated by creating classification profiles, or class maps. Packets arriving at the device are checked against the match criteria of the classification profile to determine if the packet belongs to that class. Matching traffic is subjected to the actions defined in an action profile, or policy map.

Note There is no QoS support for all the IOT services.

To configure classification profiles and action profiles, choose **Configuration > QoS > Profiles** in the left sidebar.

This section includes the following topics:

- Create a QoS Classification Profile, on page 437
- Create a QoS Action Profile, on page 440
- Check Which QoS Profiles are Configured on a Device, on page 445
- Apply a QoS Action Profile to Interface(s), on page 445
- Import QoS Profiles Discovered from Devices, on page 446
- Dissociate a QoS Action Profile from Multiple Interfaces, on page 447
- Delete QoS Classification and Action Profiles from Devices, on page 447

Create a QoS Classification Profile

Create classification profiles (class maps) to differentiate traffic into different classes so that certain actions can be applied to traffic that matches the classification criteria.

To create a classification profile:

Step 1 Choose **Configuration > QoS > Profiles** in the left sidebar.

Step 2 Click the Add (“+”) icon at the top of the Global QoS Classification Profiles pane.

Step 3 Enter a unique name for the classification profile. The name should reflect the classification criteria defined in the profile for easy identification. For further clarification, you can add a description.

Step 4 Define the matching criteria for the profile:

- Match All—All the classification criteria must be met in order for the traffic to belong to this class.

- Match Any—Any of the classification criteria can be met in order for the traffic to belong to this class.

Step 5 Under QoS Classifications, click the plus icon to define classification criteria for the classification profile.

Step 6 Select an action based on which the traffic will be classified, then click in the Value column and provide the relevant value, as follows:

Action	Description	Value
ACL	The packet must be permitted by the specified access control list (ACL).	The name of the ACL. A string of up to 32 alphanumeric characters.
MPLS - Imposition	The experimental (EXP) bit value on the imposed label entry of the packet must match the MPLS EXP value that you specify. Use either the MPLS Imposition or the MPLS Topmost for matching criteria. Once you have used one of the MPLS criteria, the other one will no longer be available.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
MPLS - Topmost	The experimental (EXP) bit value in the topmost label must match the MPLS EXP value that you specify.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
Cascade	This action is used to cascade one class map into another. It can be used when creating a new class map which has classification policies similar to an existing class map.	Reference the child class map.
QoSClassification - COS	The packet's layer 2 class of service (CoS) bit value must match the specified CoS value.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
QoSClassification - COS - Inner	The specified value must match packet's inner CoS value of QinQ packets for Layer 2 class of service (CoS) marking.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
QoSClassification - DSCP	The packet IP differentiated service code point (DSCP) value must match one or more of the specified values.	Valid values are from 0 to 63. Up to 8 comma-separated values can be entered.
QoSClassification - DSCP - IPv4 only	Match DSCP values for IPv4 packets.	Valid values are from 0 to 63. Up to 8 comma-separated values can be entered.
QoSClassification - Precedence	The packet IP precedence value must match one or more precedence values.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
QoSClassification - Precedence - IPv4 only	Match precedence values for IPv4 packets.	A number from 0 to 7. Up to 8 comma-separated values can be entered.
QoSClassification - DEI	Drop eligible indicator (DEI) is used to indicate frames eligible to be dropped when there is congestion. The packet must match the DEI value specified.	0 or 1.

Action	Description	Value
QoS-Group	The packets must be permitted based on the selected QoS group.	Up to 8 comma separated unique values ranging from or 0-55 or 0-99 or 0-511 based on the selected device. Ensure that the value you enter is supported on the device.
QoSClassification - Service Instance	Service Provider configurations have various service instances on the Provider Edge (PE) routers. QoS policy-maps are applied on these service instances or group of service instances. **Note** This criteria is applicable only on Cisco ASR 903.	Accepts any number of comma separated values ranging from 1-8000 and/or hyphenated value with each ranging from 1-8000.
QoSClassification - VLAN	Match and classify traffic on the basis of the virtual local-area network (VLAN) identification number. **Note** Click the + icon to add more than one QOS Classification - VLAN and specify values.	Accepts any number of comma separated values ranging from 1-4095 and/or hyphenated value with each ranging from 1-4095.
QoSClassification - VLAN - Inner	Match and classify traffic on the basis of the inner virtual local-area network (VLAN) identification number. **Note** Click the + icon to add more than one QOS QOS classifcation -VLAN-inner lines and specify values.	Accepts any number of comma separated values ranging from 1-4095 and/or hyphenated value with each ranging from 1-4095.
QoSClassification - Discard Class	Indicates that packets must be permitted/discarded based on the selected discard class.	Accepted value is any number between 0-7.
QoSClassification - Traffic Class	Traffic class of the QoS configuration.	Accepted value is any number between 0-7.

Step 7 Define additional QoS classifications, as required.

Step 8 Click the **Save** button at the bottom of the window to save the profile. A notification in the bottom right corner will confirm that the profile has been saved and the profile will appear in the list of profiles on the left.

Step 9 Select the profile from the list and click the **Deploy** button to initiate deployment of the profile to devices.

Step 10 If you want to create a new profile with the details of an existing Classification Profile , click the **Clone** button. This profile will have the name of the classification profile that you cloned from, and the suffix **-clone**. You can edit the name, matching criteria and any other details of this cloned profile.

Step 11 If you want the selected profile to override any other class map that already exists on the device, check the **Override existing configuration** check box. If this check box is not checked, the profile will be merged with the configurations on the device.

Step 12 Select the device(s) to which you want to deploy the QoS Classification profile.

Step 13 Schedule the deployment, if required.

Step 14 Click **Submit**. A notification in the bottom right corner will confirm that the profile has been deployed. To check the status of the deployment job, choose **Administration > Job Dashboard** from the left sidebar. Select the relevant job to view the job details and history in the lower section of the window. Click the Information icon for further details.

Create a QoS Action Profile

Create action profiles (policy maps) to specify the actions to be applied to traffic belonging to a specific traffic class.

To create an action profile:

Step 1 Choose **Configuration > QoS > Profiles** from the left sidebar.

Step 2 From the QoS Profiles pane on the left, choose, **User Defined Global QoS Profiles > Action Profiles**.

Step 3 Click the Add ("+") icon at the top of the Create Action Profile pane

Step 4 Enter a unique name for the action profile, and enter a description, if required.

Step 5 Select the classification profiles for which you want to assign actions. Under Classification Profiles, click the plus icon, select the required profile(s) from the list, and click **OK**.

Step 6 Select the Classification Profile (class map) and define the actions to be applied if traffic matches the profile. You can define Policing, Marking, Queuing, Shaping, RED actions, and Service Policy (H-QoS). There is a tab for each of these action types and its definitions, as follows:

- **Policer Action:** Traffic policing manages the maximum rate of traffic allowed on an interface through a token bucket algorithm. Traffic policing also provides a certain amount of bandwidth management by allowing you to set the burst size (Bc) for the CIR. When the peak information rate (PIR) is supported, a second token bucket is enforced and this two-rate policer can meter traffic at two independent rates: the committed information rate (CIR) and the peak information rate (PIR). The committed token bucket can hold bytes up to the size of the committed burst (bc) before overflowing and determines whether a packet conforms to or exceeds the CIR. The peak token bucket can hold bytes up to the size of the peak burst (Be) before overflowing, and determines whether a packet violates the PIR. Different actions can be taken if a packet conforms, exceeds, or violates the CIR/PIR. For instance, packets that conform can be configured to be sent, packets that exceed can be configured to be sent with a decreased priority, and packets that violate can be configured to be dropped.

  In the Policer Action tab, specify the following:

  - Committed Information Rate (CIR)—The long-term average transmission rate, specified in bits per second (bps) or as a percentage of the available or unused bandwidth. Traffic that falls under this rate will always conform. Ensure that the CIR value you enter is supported on the device and choose the right CIR unit value (bps, kbps, mbps, gbps, or percent).
  - Burst (Bc)—How large traffic bursts can be (in bytes) before some traffic exceeds the CIR.
  - Peak Information Rate (PIR)—How much traffic bursts can peak before some traffic exceeds the PIR value associated with the CIR. Ensure that the PIR value you enter is supported on the device and choose the same unit value you chose for CIR (bps, kbps, mbps, gbps, or percent).
  - Excess Burst (Be)—How large traffic bursts can be (in bytes) before traffic exceeds the PIR.
  - Under Traffic Coloring Behavior, select the action to be performed if the traffic conforms, exceeds, or violates the rate limit. Provide values as required. To enable color-aware traffic policing specify the Conform Color and Exceed Color values by associating them with respective class profiles. With color-aware policing, the

following results occur based on the CIR, the PIR, and the conform actions, exceed actions, and violate actions:

- Packets that have metering rates less than or equal to the CIR and belong to the specified class (conform-color) are policed as conforming to the rate. These packets are also policed according to the conform action specified. In this instance, the packets will be transmitted.
- Packets that have metering rates between the CIR and the PIR and belong to either to the conform-color class or exceed-color class are policed as exceeding the CIR. These packets are also policed according to the exceed action specified. In this instance, the precedence value of the packets will be set and the packets transmitted.
- Packets that have metering rates higher than the PIR or belong to neither class conform-color or class exceed-color are policed as violating the rate. These packets are also policed according to the violate action specified. In this instance, the packets will be dropped.

- **Marker Action:** Packet marking allows you to partition your network into multiple priority levels or classes of service. Marking of a traffic flow is performed by:
  - Setting IP Precedence or DSCP bits in the IP Type of Service (ToS) byte .
  - Setting CoS bits in the Layer 2 headers.
  - Setting EXP bits within the imposed or the topmost Multiprotocol Label Switching (MPLS) label.
  - Setting qos-group, traffic-class, and discard-class bits.

  In the Marker Action tab, specify the following:
  - Marking Feature and Marking Value—The method by which the traffic will be marked, and the required value.

- **Queueing Action:** Queueing is used for traffic congestion management. It entails the creation of queues, assignment of packets to those queues based on the classification of the packet, and scheduling of the packets in a queue for transmission.

  In the Queueing Action tab, select the method by which traffic will be queued, either Bandwidth or Priority, then specify the following:
  - Bandwidth—The amount of bandwidth to be assigned to the traffic class, either in kilobits per second, or as a percentage of absolute guaranteed bandwidth. If you selected to queue by bandwidth, you can also assign bandwidth as a percentage of remaining bandwidth.
  - Queue Limit— The maximum number of packets/bytes/milliseconds for all the individual queues associated with this class. When the queue size exceeds this value, packets will be dropped.

  If you selected Bandwidth, specify the following:
  - Enable Fair Queue—Check the check box to enable weighted fair queueing

    .
  - Individual Queue Size—Relevant if fair queueing is enabled. Specify the maximum number of packets allowed in each per-class queue during periods of congestion.

  If you selected Priority, specify the following:

- Queue Burst Size (bytes)—The burst size configures the network to accommodate temporary bursts of traffic. Range is 18 to 2000000 bytes. Default is 200 milliseconds of traffic at the configured bandwidth rate.
- Priority Level—Classes under a policy map can have different priority, from priority queue level 1 to 3. Packets on these queues are subjected to less latency with respect to other queues. You cannot specify the same priority level for two different classes in the same policy map.

- **Shaping Action:** Traffic shaping regulates traffic by shaping it to a specified rate.

  In the Shaping Action tab, specify the following:

  - Select Average or Peak rate traffic shaping—Average rate shaping limits the transmission rate to the CIR. Peak rate shaping configures the router to send more traffic than the CIR. To determine the peak rate, the router uses the following formula: peak rate = CIR(1 + Be / Bc) where Be is the Excess Burst size and Bc is the Committed Burst size.
  - If you selected Peak rate traffic shaping, specify the burst size and the excess burst size in bytes.
  - If required, enable FECN Adaptive Shaping. Adaptive shaping estimates the available bandwidth when backward explicit congestion notification (BECN) signals are received. With FECN adaptive shaping, the router reflects forward explicit congestion notification (FECN) signals as BECN signals.
  - If FECN Adaptive Shaping is enabled, specify the Adaptive Rate, which is the minimum bit rate to which the traffic is shaped.

- **RED Action:** Weighted Random Early Detection (WRED) is a congestion avoidance technique that implements a proactive queuing strategy that controls congestion before a queue reaches its queue limit. WRED combines the capabilities of the random early detection (RED) mechanism with IP precedence, differential services code point (DSCP), and discard-class to provide preferential handling of higher priority packets. When an interface starts to become congested, WRED discards lower priority traffic with a higher probability. WRED controls the average depth of Layer 3 queues.

  In the RED Action tab, specify the following:

  - Classification Mechanism—Select the basis upon which the WRED drop policies are defined. For WRED, you define drop policies based on specific packet classification, as follows:

    CLP—Configures a drop policy for WRED based on a cell loss priority (CLP) value. Valid values are 0 or 1.

    CoS—Configures a drop policy for WRED based on the specified class of service (CoS) bit associated with the packet. Valid values are from 0 to 7.

    Discard Class—Configures a drop policy for WRED based on a discard-class value. Valid values are from 0 to 7. The discard-class value sets the per-hop behavior (PHB) for dropping traffic. WRED based on discard-class is an egress function.

    DSCP—Configures a drop policy for WRED based on a DSCP value. When configured, the router randomly drops packets with the specified DSCP value, according to the WRED thresholds you configure.

    Precedence—Configures a drop policy for WRED based on an IP precedence level. Valid values are from 0 to 7, where 0 typically represents low priority traffic that can be aggressively managed (dropped) and 7 represents high priority traffic. Traffic at a low precedence level typically has a higher drop probability. When WRED drops packets, source hosts using TCP detect the drops and slow the transmission of packets.

    DEI—The discard eligibility (DE) bit in the address field of a frame relay frame is used to prioritize the discarding of frames in congested frame relay networks. The frame relay DE bit has only one bit and therefore

only has two settings, 0 or 1. If congestion occurs in a frame relay network, frames with the DE bit set at 1 are discarded before frames with the DE bit set at 0.

RED Default—The default set of minimum thresholds, maximum thresholds, and Mark Probability Denominator (MPD) settings for a class in the WRED profile.

- If required, enable ECN. ECN (Explicit Congestion Notification) marks packets instead of dropping them when the average queue length exceeds a specific threshold value. Routers and end hosts use this marking as a signal that the network is congested and slow down packet transmission.
- Define the thresholds and mark probability per valid value of the selected classification mechanism. For example, if you are using Precedence, you can define thresholds for each of the 7 valid values. The minimum threshold is the minimum number of packets allowed in the queue. When the average queue length reaches the minimum threshold, WRED randomly drops *some* packets with the specified DSCP, IP precedence, discard-class, or atm-clp value. Valid minimum threshold values are from 1 to 16,384. The maximum threshold is the maximum number of packets allowed in the queue. When the average queue length exceeds the maximum threshold, WRED drops all packets with the specified DSCP, IP precedence, discard-class, or atm-clp value. Valid maximum threshold values are from the value of the minimum threshold to 16,384.

- **Service Policy:**

  Using the Service Policy tab, you can configure Hierarchical QoS (H-QoS) which enables you to specify QoS behavior at multiple levels of hierarchy. You can use H-QoS to specify multiple policy maps to shape multiple queues together. All hierarchical policy types consist of a top-level parent policy and one or more child policies. The service-policy command is used to apply a policy to another policy, and a policy to an interface.

  To configure H-QoS, navigate to the **Service Policy** tab, select the **Enable** check box, and use the **Service Policy** drop-down menu to select the child service policy. The selected child service policy will be associated to the parent policy map that this action profile belongs to. Note that a child service policy cannot act as a parent policy of the same policy map. For example, if a child service policy called X belongs to a parent policy map Y, then the child policy X cannot contain the service policy map Y.

  H-QoS Limitations: On Cisco IOS-XE devices such as Cisco ASR903, Cisco ASR907, Cisco ASR920, and Cisco NCS42XX, the following H-QoS limitations are applicable:

  - Parent policy map limitations:
    - A parent policy map can be created only using the 'class-default' class.
    - The parent policy map must contain a class with matching criterion such as an EFP (service instance).
    - The parent policy map must contain a class with matching criterion such as VLANs.
  - Child policy map limitations:
    - Child policy maps cannot be created with EFP (service instance) and VLAN as the match-type.

Step 7 Click the **Save** button at the bottom of the window to save the profile. A notification in the bottom right corner will confirm that the profile has been saved and the profile will appear in the list of profiles on the left.

Step 8 From the Global QoS Action Profiles pane, select the profile, and click the **Deploy** button to initiate deployment of the profile to devices.

Step 9 If you want to create a new profile with the details of an existing Action Profile , click the **Clone** button. This profile will have the name of the action profile that you cloned from, and the suffix **-clone**. You can edit the name, actions and any other details of this cloned profile.

Step 10 If you want the selected profile to override any other policy map that already exists on the device, check the **Override existing configuration** check box. If this check box is not checked, the profile will be merged with the configurations on the device.

Step 11 Select the device(s) to which you want to deploy the QoS Action profile.

Step 12 Schedule the deployment, if required.

Step 13 Click **Submit**. A notification in the bottom right corner will confirm that the profile has been deployed. To check the status of the deployment job, choose **Administration > Job Dashboard** from the left sidebar. Select the relevant job to view the job details and history in the lower section of the window. Click the Information icon for further details.

Create a QoS Sub-Action Profile

An action profile (policy map) specifies the actions to be applied to traffic belonging to a specific traffic class. They are associated with multiple Classification Profiles that define the actions to be applied if traffic matches the profile. You can define Policing, Marking, Queuing, Shaping, RED actions, and Service Policy (H-QoS).

Sub-action profiles are action profiles that are associated with only a single classification profile. You can use sub-action profiles during circuit/VC provisioning to associate a singular action based action profile with the Circuit/VC.

To create a sub-action profile:

Step 1 Choose **Configuration > QoS > Profiles** from the left sidebar.

Step 2 From the QoS Profiles pane on the left, choose, **User Defined Global QoS Profiles > Sub-Action Profiles**.

Step 3 Click the Add (“+”) icon at the top of the Create Sub-Action Profile pane

Step 4 Enter a unique name for the sub-action profile, and optionally enter a description.

Step 5 Select the classification profile for which you want to assign actions. Under Classification Profiles, click the plus icon, select the required profile from the list, and click **OK**.

You can add only a single classification profile to a sub-action profile. To associate multiple classification profiles, you must create an action profile.

Step 6 Specify the required actions that need to be taken when the traffic matches the criteria specified in the classification profiles. For a description of the various options, see, Create a QoS Action Profile, on page 440.

Import and Export QoS Action and Sub-Action Profiles

Step 1 Choose **Configuration > QoS > Profiles** from the left sidebar.

Step 2 To export Action Profiles, choose, **User Defined Global QoS Profiles > Action Profiles** from the pane on the left.

Step 3 To export Sub-Action Profiles, choose, **User Defined Global QoS Profiles > Sub-Action Profiles** from the pane on the left.

Step 4 To export profiles, select the profiles that you want to export and click **Export**. The files are saved in the location that you specify.

Step 5 To import profiles, click **Import**, choose the XML files (that contain information about the action or sub-action profiles) that you want to import, and click **OK**. The imported profiles are listed under the Action Profiles or Sub-Action Profiles pages respectively.

Please note:

- Although there is no limit to the number of profiles you can import in a single instance, we recommend that you choose a maximum of 10 profiles to ensure optimal performance.
- Ensure that the size of the file you want to import is below 20 MB.
- Files of only xml format can be imported.

Check Which QoS Profiles are Configured on a Device

To see the QoS profiles that have been deployed to a specific device:

Step 1 Choose **Configuration** > **Network** > **Network Devices** from the left sidebar.

Step 2 Locate the required device and click on the device name hyperlink to display the device details.

Step 3 Click the **Device Details** tab.

Step 4 Click on the arrow next to QoS in the left pane, and select either **Action Profiles** or **Classification Profiles**. A table listing the profiles that have been deployed to the selected device is displayed. Click on the profile name (blue hyperlink) to display the details of the profile.

Apply a QoS Action Profile to Interface(s)

You can select an action profile deployed to a device and apply it to multiple interfaces on that device. An action profile enables you to specify the actions to be applied to traffic belonging to a specific traffic class. Before applying an existing profile to interfaces, you can modify the profile or use it to create a new profile. When you choose an interface that has an action profile already applied to it, Cisco EPN Manager notifies you about it and enables you to override the existing profile. To be able to apply an action profile to interfaces, you first need to ensure that the required profile has been deployed to the device. To do this, see Create a QoS Action Profile, on page 440.

To apply an action profile to interfaces:

Step 1 Choose **Configuration > QoS > Interfaces** from the left sidebar.

Cisco EPN Manager interfaces are displayed under the categories **Ethernet CSMACD, IEEE8023 ADLAG**, **Gigabit Ethernet**, and **L2 VLAN**. All other ports are displayed under the **User Defined** category.

Step 2 Select the interfaces that you want to associate to an Action profile.

Step 3 Click **Associate Action Profile** to select the action profile and to set the direction in which it must be applied. The available action profiles list and the interfaces it can be applied to are listed. The interfaces are listed by their name, application direction, and the action profiles that already exist on the interface.

Note QoS scaling profile configuration is the prerequisite to associate action profiles for Bundle-ethernet interfaces and subinterfaces. Configuration example:

```
hw-module profile qos bundle <high-scale|medium-scale|low-scale> location <card>
```

Step 4 Select the required action profile from the **Action Profiles** drop-down menu. If the menu is empty, you need to create action profile and then try to associate them with devices. See, Create a QoS Action Profile, on page 440.

Step 5 In the **Interfaces** section, specify the direction in which the profile is to be applied. While applying a profile to a subinterface, ensure that it is applied in a direction opposite to that of the main interface. To change the applied direction, use the **Edit** icon at the top left corner of the dialog.

Note Policy Maps that contain queuing actions cannot be applied to interfaces in Ingress direction.

Step 6 (Optional) You can also schedule the application of the selected action profile to a later date and time. To do this, expand the **Schedule** section and specify the date and time and frequency for when you the profile to be applied. This task can further be edited on the Jobs page if required.

Step 7 Click **OK** to apply the action profile to the selected devices. A notification at the bottom right corner of the dialog will confirm whether the profile has been successfully applied or if the job failed. Click the **Show Details** link for more information.

To dissociate action profiles from the interfaces they are applied to, see Dissociate a QoS Action Profile from Multiple Interfaces, on page 447

Import QoS Profiles Discovered from Devices

You can import QoS profiles discovered from the device directly into Cisco EPN Manager. Once the QoS profiles are imported, they can be edited and further configured on the device using Cisco EPN Manager. Profiles which are discovered from the device with profile names that match other profiles already present in Cisco EPN Manager are represented as Global profiles. This is indicated in the Global column in the Global Profiles page. Note that Global profiles could have the same names but different QoS configuration. While importing global profiles, you can choose to either overwrite the existing profile (with the same name) using the discovered profile or you can rename the profile before you import it.

To import QoS profiles discovered from devices:

Before you begin

Ensure that the device's Inventory Collection status is Completed. This ensures that the QoS profiles from the devices are discovered by Cisco EPN Manager.

Step 1 Choose **Configuration > QoS > Profiles** from the left sidebar to display all Cisco EPN Manager QoS profiles.

Step 2 To import Action profiles, from the QoS Profiles pane on the left, choose, **Discovered Profiles** > **Action Profiles**.

Step 3 To import Classification profiles, from the QoS Profiles pane on the left, choose, **Discovered Profiles** > **Classification Profiles**.

Step 4 To first select a device and choose the profiles discovered on that device:

a) Choose **Configuration** > **Network** > **Network Devices**, and select the device by clicking the device's Name hyperlink.
b) Click the **Device Details** tab.
c) Expand **QoS**.
d) Choose **Action Profiles** or **Classification Profiles** based on the type of profile you want to import from the device.
e) (Optional) After viewing the profiles, to import these profiles directly from the page that lists all QoS profiles discovered by Cisco EPN Manager, click the **Global Profile Page** hyperlink, and skip to Step 5.
f) Select the profiles and click **Make Global**.

g) Go to Step 6.

Step 5 Select the profiles that you want to import and click **Import**. To ensure that you are importing profiles that are not already present on the device, choose profiles that are not Global (marked as No in the Global column).

Step 6 If there are duplicate profiles present in Cisco EPN Manager, you are asked to either rename the profile to create a profile with a new name and the same QoS configuration or overwrite the existing profile. Make the required changes.

Step 7 If you want to create a new profile with the details of an existing QoS Profile , click the **Clone** button. This profile will have the name of the QoS profile that you cloned from, and the suffix **-clone**. You can edit any details of this cloned profile.

Step 8 Click **Save** to import the selected QoS profiles.

To apply the imported profiles to a given device's interfaces, see, Apply a QoS Action Profile to Interface(s), on page 445.

Dissociate a QoS Action Profile from Multiple Interfaces

An action profile enables you to specify the actions to be applied to traffic belonging to a specific traffic class. You can select an action profile deployed to a device and apply it to multiple interfaces on that device. After you have applied the profile to the interfaces, you can choose to dissociate them from those interfaces if required. To dissociate an action profile from interfaces, you first need to ensure that the required profile has been applied to the device. See Apply a QoS Action Profile to Interface(s), on page 445.

To apply an action profile to interfaces:

Step 1 Choose **Configuration** > **QoS** > **Interfaces** from the left sidebar.

Alternatively, you can navigate to **Configuration > QoS > Profiles** to first select the profile before dissociating it from the interfaces it is applied to.

Cisco EPN Manager interfaces are displayed under the categories **Ethernet CSMACD, IEEE8023 ADLAG**, and **L2 VLAN**. All other ports are displayed under the **User Defined** category.

Step 2 Select the interfaces from which you want to dissociate the action profile.

Step 3 Click **De-associate Action Profile**.

Step 4 (Optional) You can also schedule the de-association of action profiles to a later date and time. To do this, expand the **Schedule** section and specify the date, time, and frequency based on which the profiles must be dissociated.

Step 5 Click **OK** to confirm. The selected interfaces are dissociated from the action profiles that were applied to them. A notification at the bottom right corner of the window will confirm whether the profile has been successfully dissociated or if the job failed. Click the **Show Details** link for more information.

Delete QoS Classification and Action Profiles from Devices

To delete QoS classification and action profiles that are deployed to devices, navigate to the paths listed in the table below.

Note You cannot delete QoS action and classification profiles discovered directly from the device. Only profiles created using (and imported into) Cisco EPN Manager can be deleted.

In order to avoid deletion of referenced profiles, the delete operation is not supported in the following scenarios:

- You cannot delete QoS classification profiles associated with other classification profiles. For example if a classification profile uses the Cascade option to reference the selected classification profile, then the delete operation for the selected profile will fail.
- You cannot delete a QoS classification profiles referenced by an action profile.
- Action profiles successfully applied to device interfaces cannot be deleted.
- An action profile cannot be deleted if it is referenced by another action profile. For example, if action profiles are associated to other action profiles by use of a reference policy, then the delete operation of such action profiles fails.

Table 30: Navigation paths to delete QoS action and classification profiles

Task	Steps in the GUI
Delete user defined classification profiles	**1.** Choose **Configuration > QoS > Profiles > User Defined Global QoS Profiles > Classification Profiles**. **2.** Select the classification profile you want to remove from the devices as well as from Cisco EPN Manager. **3.** Click the **X** (delete) icon in the task bar. **4.** Alternatively, you can click the device hyperlink to choose the devices from which the selected classification profile must be deleted. **5.** Click **Submit**. You can view the status of the delete operation by clicking the Job Details pop up window.
Delete user defined action profiles	**1.** Choose **Configuration > QoS > Profiles > User Defined Global QoS Profiles > Action Profiles**. **2.** Select the action profile you want to remove from the devices as well as from Cisco EPN Manager. **3.** Click the **X** (delete) icon in the task bar. **4.** Alternatively, you can click the device hyperlink to choose the devices from which the selected action profile must be deleted. **5.** Click **Submit**. You can view the status of the delete operation by clicking the Job Details pop up window.

Save Your Device Changes

After you make a change to a device, save your changes to the database and, if desired, collect the device's physical and logical inventory. See these topics for more information:

- Save Device Configuration Changes to the Database (Update), on page 449
- Collect a Device's Inventory Now (Sync), on page 449

Save Device Configuration Changes to the Database (Update)

After making a change to your devices, you should save those changes to the database by clicking **Update** in the configuration window. If an Update button is not provided, perform a manual *sync* which will save your changes, but also collect the device's physical and logical inventory and save it to the database. See Collect a Device's Inventory Now (Sync), on page 449

Collect a Device's Inventory Now (Sync)

The Sync operation performs an immediate inventory collection for a device. When it performs a Sync, Cisco EPN Manager collects the selected device's physical and logical inventory and synchronizes the database with any updates. If you do not perform a Sync operation after making a change to a device, your change will not be saved to the database until the daily inventory collection.

Note The Sync operation is different from the Update operation. Update saves configuration changes without performing an inventory collection. If you want to use Update instead of Sync, see Save Device Configuration Changes to the Database (Update), on page 449.

Note This Sync operation is different from working with *out-of-sync device configuration files*. An out-of-sync device is a device that has a startup configuration files that is different from its running configuration file. For more information, see Synchronize Running and Startup Device Configurations, on page 121.

Use one of these methods to perform a manual Sync.

To collect the inventory for:	Do the following:
A single device	• From the device's Device 360 view, choose **Actions** > **Sync Now**. **Note** You can view the status of the sync operation on the device. For more information, see Device Sync State, on page 450. • From the Network Devices table, check the device's check box, then click **Sync**.
Multiple devices	From the Network Devices table, select the devices (by checking their check boxes), then click **Sync**.

Device Sync State

Device Sync State—Indicates status of the Sync operation performed on a device.

Table 31: Device Sync State

Icon	Device Sync State	Description
	Synchronizing	Device synchronization is in progress.
	Completed	Device synchronization completed successfully.
	Error/Warning	List of errors or warnings indicated: • Add Initiated • Collection Failure • Completed with Warning • Delete In Progress • In Service • In Service Maintenance • No License • Partial Collection Failure • SNMP Connectivity Failed • SNMP User Authentication Failed • Switch Port Trace • Wrong CLI Credentials

Note In Service Maintenance filter is not available for Last inventory collection status.

Launch Cisco Transport Controller to Manage Cisco NCS and Cisco ONS Devices

The Cisco Transport Controller (CTC) is the software interface for a subset of Cisco ONS and Cisco NCS devices. CTC is a Java application that resides on the control cards. It is used to provision and administer these devices.

You can launch CTC from Cisco EPN Manager. Only the latest CTC release is launched, regardless of the NE release you selected. If you need to use other CTC releases, launch CTC from a web browser and connect directly to the NE that has the required CTC release.

To launch CTC:

Before you begin

Make sure the devices are properly configured to launch CTC. See Configure Devices So They Can Be Modeled and Monitored, on page 53.

Step 1 From the left sidebar, choose **Inventory > Device Management > Network Devices**.

Step 2 Click the "**i**" icon next to the Cisco ONS or Cisco NCS device's IP address to launch the Device 360 view.

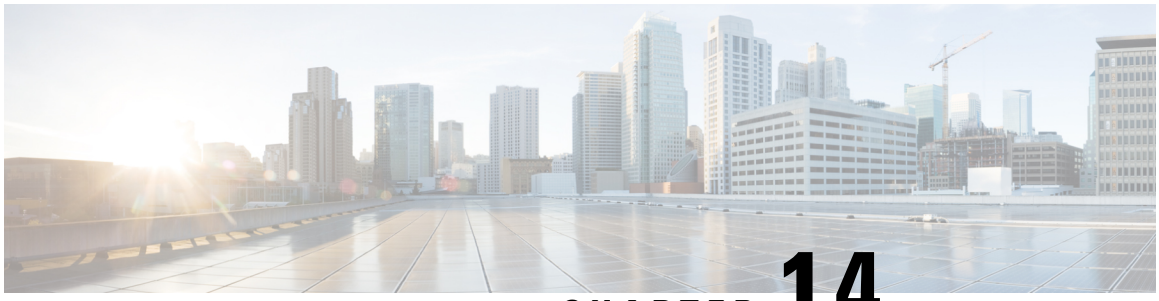
Step 3 In the Device 360 view, choose **Actions > Launch CTC**. The CTC launcher application is downloaded to your computer. Note that this action will be disabled if launching CTC is not supported on the selected device type.

Step 4 In the CTC Launcher window, choose one of the following connection mode:

- Use IP—Connection to the device is established using the device's IP address (default option).
- Use TL1 Tunnel—Connection to the device is established using a TL1 session. You can start a TL1 session from CTC or use a TL1 terminal. Note- Use this option to connect to the device that resides behind the third-party OSI-based GNE. The CTC launcher creates a TL1 tunnel to transport the TCP traffic through the OSI-based GNE and the provisioning occurs in CTC

Step 5 Select the CTC Version, and then click **Launch CTC**.

Step 6 Enter your CTC credentials.



CHAPTER 14

Create Templates To Automate Device Configuration Changes

This chapter has the following topics.

Why Create New Configuration Templates?

Cisco EPN Manager provides a number of out-of-the-box configuration templates that you can use to make changes on your network devices. Those are described in Create a New CLI Configuration Template Using An Existing Template, on page 455.

If you have sufficient privileges, you can also create new templates that meet the exact needs of your environment, and then make those templates available for others to use. You can make the templates as simple or as complex as needed, including grouping multiple templates together into a composite template. Finally, you can associate templates with particular devices by creating configuration groups.

Cisco EPN Manager provides out-of-the-box CLI commands that you can use in your templates. It also provides a blank CLI template you can use to create new CLI commands. You can use them singly or with other commands in a composite template.

How you use configuration templates can depend on factors such as how large your network is, the number of designers in your organization, and how much variation there is among devices configuration. For example:

- For a small network with only one or two designers and a limited number of device configurations, start by copying the CLI configurations you know are "good" into a set of templates. You could then combine them into composite templates and make them available to your operators.
- For a large network with many different device configurations, try to identify the configurations you can standardize. This lets you control the amount of exceptions to these standards, and lets you turn features on and off as needed.

Ways to Create Configuration Templates Using Cisco EPN Manager

Cisco EPN Manager provides different methods for creating new configuration templates, depending on your user account privileges. *CLI configuration templates* contain one or more CLI configuration commands (the same commands you would type when configuring a device). *Composite configuration templates* are comprised of two or more CLI or composite configuration templates. You can specify the order in which the commands are deployed to devices.

- Modify one of the out-of-the-box CLI templates. See Create a New Composite Template, on page 465.
- Use the blank CLI template and enter code by hand. See Create a New CLI Configuration Template Using a Blank Template, on page 454.
- Use the blank CLI template and copy and paste code from a command line configuration session, CLI script, or other stored set of configuration commands. See Create a New CLI Configuration Template Using An Existing Template, on page 455.
- Merge several existing out-of-the-box or user-defined templates into a single template. You specify the order in which the templates contained in the composite template are deployed to devices. See Create Configuration Groups for Deploying Templates to Groups of Devices , on page 467.

Once you have created a set of templates, you can export and import them.

Create a New CLI Configuration Template Using a Blank Template

Use templates to define a set of reusable device configuration commands. A description of CLI templates and how you can use them is displayed in the web GUI when you choose **Configuration** > **Templates** > **Features & Technologies**, then choose **CLI Templates**.

If you want to edit a template that is provided with Cisco EPN Manager, make a copy of the template, give it a new name, and then edit it. See Create a New CLI Configuration Template Using An Existing Template, on page 455.

Templates that you create are stored under **My Templates**.

Before you begin

Configuration templates are not supported by default on Cisco Optical Networking devices. To enable configuration templates support, select an existing pre-defined CLI configuration template, and in its Device

Type section, enable the Optical Networking checkbox. Save this CLI template as a new template. The template is now saved as a user-defined template which lists all optical networking devices such as Cisco NCS 2000, Cisco NCS 4000 devices, and so on.

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.

Step 2 Expand **CLI Templates**, then choose **CLI**.

Step 3 In the **Template Basic** area:

a) Enter a meaningful name for the template. Templates are listed alphabetically in the web GUI.

b) (Optional) Enter a short description that describes how the template should be used—for example, "enable traps on IOS devices."

c) (Optional) Tag the template with an intuitive name. For information on tags, choose **My Tags**.

d) Enter the device operating systems on which the template can be executed (for example, 12.2 or 15.3). When you execute the template, older device OS versions are filtered out. If you leave this field blank, the template will be applied all OSs for the specified devices.

Step 4 Specify the device configuration commands in the **Template Detail** area.

a) Enter or paste the copied code into the **CLI Content** field. You can copy code from a command line configuration session, CLI script, or other stored set of configuration commands. You must enter code using Apache VTL.

b) Configure your variables using the **Add Variables** dialog. Variables will prompt you for a value when you execute the template.

- To create a variable using a name in the code, select the code (no spaces) and click the + sign at the top left of the **Add Variables** area. This creates a new (unconfigured) variable by that name in the **Add Variables** dialog.
- Click the + sign at the top right of the **Add Variables** area. This adds a blank row to the **Add Variables** dialog.

For information about creating variables, see Entering Variables in a Template, on page 456.

c) To see how the variable will be displayed when the template is executed, click **Form View**.

d) To save your variables, click **Add to CLI**.

Step 5 Save your template. Click **Save as New Template**, specify the folder (in **My Templates**) in which you want to save the template, then click **Save**.

Note

a. Device configuration commands in the **Template Detail** area cannot contain special characters.

b. Entering XML specific special characters in the **Description** field under the **Template Basic** area causes the template export to fail.

Create a New CLI Configuration Template Using An Existing Template

The easiest way to create a new configuration template is to find a similar existing template, copy it, and edit it. You can also use this procedure to edit templates that you created. (You can only edit templates that you create.)

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.

Step 2 Expand **CLI Templates**, then choose **System Templates - CLI**.

Step 3 In the Template navigation panel on the left , locate the template you want to copy, hover your mouse cursor over the **i** icon that is displayed next to the template name, then click **Duplicate** in the popup window.

Step 4 In the **Duplicate Template Creation** dialog, specify a name and the folder (under **My Templates**) where you want the new template to be saved, and click **OK**.

For example, if you copy a template that resides under **CLI Templates** > **System Templates - CLI**, by default the template is saved under **My Templates** > **CLI Templates** > **System Templates - CLI (User Defined)** .

Step 5 Add the validation criteria and CLI content as described in Create a New CLI Configuration Template Using a Blank Template, on page 454 .

Entering Variables in a Template

These topics provide information that will help you when entering variables into a template:

Data Types

The following table lists data types that you can configure in the Manage Variables page.

Data Type	Description
String	Enables you to create a text box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
Integer	Enables you to create a text box that accepts only numeric value. If you want to specify a range for the integer, expand the row and configure the Range From and To fields. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
DB	Enables you to specify a database type. See the Manage Database Variables in CLI Templates, on page 457.

IPv4 Address	Enables you to create a text box that accepts only IPv4 addresses for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.
Drop-down	Enables you to create a list for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field (with a comma-separated value for multiple lists which appears in the UI).
Check box	Enables you to create a check box for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field.
Radio Button	Enables you to create a radio button for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value field.
Text Area	Enables you to create a text area which allows multiline values for CLI templates. To specify a validation expression and a default value, expand the row and configure the Default Value and Validation Expression fields.

Manage Database Variables in CLI Templates

You can use database (DB) variables for the following reasons:

- DB variables are one of the data types in CLI templates. You can use the DB variables to generate device-specific commands.
- DB variables are predefined variables. To view the list of predefined DB variables, see the CLITemplateDbVariablesQuery.properties file at the following location: folder/opt/CSCOlumos/conf/ifm/template/inventoryTagsInTemplate.
- For example, SysObjectID, IPAddress, ProductSeries, ImageVersion are DB variables.When a device is added to Cisco EPN Manager, the complete details of the device is collected in the DB variables. That is, the OID of the devices is collected in SysObjectID, product series in ProductSeries, image versions of the device in ImageVersion, and so on.
- Using the data collected by the DB variables, accurate commands can be generated to the device.
- You can select the DB variable in the Type field (using the Managed Variables page). Expand the name field and fill in the default value field with any of the DB variables which you want to use.
- When a device is discovered and added to Cisco EPN Manager, you can use the database values that were gathered during the inventory collection to create CLI templates.

Note While it is possible to create a customized query using Enterprise JavaBeans Query Language (EJB QL), only advanced developers should attempt this. We recommend you use the variables defined in the CLITemplateDbVariablesQuery.properties file only.

Use Validation Expressions

The values that you define in the Validation Expression are validated with the associated component value. For example, if you enter a default value and a validation expression value in the design flow, this will be validated during the design flow. That is, if the default value does not match with the entered value in the validation expression, you will encounter a get error at the design flow.

Note The validation expression value works only for the string data type field.

For example, choose **Configuration** > **Templates** > **Features and Technologies**, then choose **CLI Templates** > **CLI**. In the Template Detail area, click the **Add Variable** tab to view the list of Variables. Click the Add plus sign (+) in the Add Variables tab to add a row to the CLI template. Choose String in the Type field, enter the remaining values, and click **Save**. From the list of variables, expand the details of this new variable and configure the regular expression, which will not allow a space in that text box. Enter the following expression in the Validation Expression field.

```
^[\S]+$
```

Default value (optional)—ncs

The value should match with regular expression in the validation expression field.

Save the template, and then select a device. Try to enter a space in the text field. You will encounter a regular expression error.

Add Multi-line Commands

To enter multi-line commands in the CLI Content area, use the following syntax:

```
<MLTCMD>First Line of Multiline Command
Second Line of Multiline Command
......
......
Last Line of Multiline Command</MLTCMD>
```

where:

- <MLTCMD> and </MLTCMD> tags are case-sensitive and must be entered as uppercase.
- The multi-line commands must be inserted between the <MLTCMD> and </MLTCMD> tags.
- The tag cannot be started with a space.
- The <MLTCMD> and </MLTCMD> tags cannot be used in a single line.

Example 1:

```
<MLTCMD>banner_motd Welcome to
Cisco. You are using
Multi-line commands.
</MLTCMD>
```

Example 2:

```
<MLTCMD>banner motd ~ ${message}
</MLTCMD>
```

where {message} is a multi-line input variable.

Restrictions for Using Multi-Line Banner Commands

Cisco EPN Manager does not support multi-line banner commands. You can use *banner file xyz format* as shown in the following example.

```
#conf t
Enter configuration commands, one per line. End with Ctrl-Z.
(config)#parameter-map type webauth global
(config-params-parameter-map)# type webauth
(config-params-parameter-map)#banner file tftp://209.165.202.10/banner.txt
(config-params-parameter-map)#^Z
#more tftp://192.168.0.0/banner.txt
Disclaimer:
Usage of this wireless network is restricted to authorized users only.
Unauthorized access is strictly forbidden.
All accesses are logged and can be monitored.
#
```

Add Enable Mode Commands

Use this syntax to add enable mode commands to your CLI templates:

```
#MODE_ENABLE<<commands >>#MODE_END_ENABLE
```

Add Interactive Commands

An interactive command contains the input that must be entered following the execution of a command.

To enter an interactive command in the CLI Content area, use the following syntax:

```
CLI Command<IQ>interactive question 1<R>command response 1 <IQ>interactive question
2<R>command response 2
```

where <IQ> and <R> tag are case-sensitive and must be entered as uppercase.

For example:

```
#INTERACTIVE
crypto key generate rsa general-keys <IQ>yes/no<R> no
#ENDS_INTERACTIVE
```

Note You must replace the <IQ> tag with the <IQNONEWLINE> tag for any interactive questions in which the default <return> or newline character is not required in the command for any of the controller devices. For example,

```
#INTERACTIVE
transfer download start <IQNONEWLINE>y/N<R>y<IQNONEWLINE>y/N<R>y
#ENDS_INTERACTIVE
```

Note The <IQ> tag utilizes regular expressions for interactive questions. You must use the valid regular expressions for matching patterns.

Format

```
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
```

Example for invalid content used in interactive question

```
#INTERACTIVE
save config<IQ>Are you sure you want to save? (y/n)<R>y
#ENDS_INTERACTIVE
```

Using the Question Mark "?" in between is invalid and does not match the pattern.

Example for valid content used in interactive question

```
#INTERACTIVE
save config<IQ>(y/n)<R>y
#ENDS_INTERACTIVE
```

Combining Interactive Enable Mode Commands

Use this syntax to combine interactive Enable Mode commands:

```
#MODE_ENABLE
#INTERACTIVE
commands<IQ>interactive question<R>response
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

For example:

```
#MODE_ENABLE
#INTERACTIVE
mkdir <IQ>Create directory<R>XXX
#ENDS_INTERACTIVE
#MODE_END_ENABLE
```

Adding Interactive Multi-line Commands

This is an example of an interactive command that contains multiple lines:

```
#INTERACTIVE
macro name EgressQoS<IQ>Enter macro<R><MLTCMD>mls qos trust dscp
wrr-queue queue-limit 10 25 10 10 10 10 10
```

```
wrr-queue bandwidth 1 25 4 10 10 10 10
priority-queue queue-limit 15
wrr-queue random-detect 1
wrr-queue random-detect 2
wrr-queue random-detect 3
wrr-queue random-detect 4
wrr-queue random-detect 5
wrr-queue random-detect 6
wrr-queue random-detect 7
wrr-queue random-detect max-threshold 1 100 100 100 100
wrr-queue random-detect min-threshold 1 80 100 100 100
wrr-queue random-detect max-threshold 2 100 100 100 100
wrr-queue random-detect min-threshold 2 80 100 100 100
wrr-queue random-detect max-threshold 3 80 90 100 100
wrr-queue random-detect min-threshold 3 70 80 90 100
wrr-queue random-detect min-threshold 4 70 80 90 100
wrr-queue random-detect max-threshold 4 80 90 100 100
wrr-queue random-detect min-threshold 5 70 80 90 100
wrr-queue random-detect max-threshold 5 80 90 100 100
wrr-queue random-detect min-threshold 6 70 80 90 100
wrr-queue random-detect max-threshold 6 80 90 100 100
wrr-queue random-detect min-threshold 7 60 70 80 90
wrr-queue random-detect max-threshold 7 70 80 90 100
@</MLTCMD>
#ENDS_INTERACTIVE
```

Use Global Variables in a Template

Cisco EPN Manager enables you to deploy customized CLI configuration to your devices by creating CLI templates which contain these customized configuration options. When you create CLI templates or modify existing ones, you can define the content of the template using global and/or template variables.

- Template variables: allow you to input values to the variable during CLI template or service creation.
- Global variables: are predefined and associated with the CLI template or with a service at a global level (by default). You cannot view a global variable or input its values during service creation.

All variables names start with words that identify them as global or template variable. Global variables are accessible to all Cisco EPN Manager templates such as CLI templates or Composite templates. They identify the type of service (CE, L3VPN, CEM, etc.) that the variable can be associated with. If you create a new global variable, you must ensure that you specify a name that starts with the letters 'gv' followed by other words that promote easy identification of the variable. Global variables that you create, can be further edited and deleted. The global variables available in Cisco EPN Manager by default, cannot be edited or deleted. While global variables are applicable to all template types, the variables created specifically during CLI template creation are applicable to that template alone. These variables created during CLI template creation cannot be associated with other CLI templates.

In the CLI template configuration example shown below, 'gv.service-ethernet-maintInterfaceName' represents the global variable. If this template is associated with a service, then during service creation, the dynamic part of the global variable, 'mainInterfaceName', is replaced by the values (such as the ethernet interface, in case of CE services) specified in the service. However, you will not be able to view or modify this global variable during service creation. '$descr' is a static value which represents the template variable. During service creation, this template variable will enable you to modify or specify a value of the type String (for the description field).

```
interface $gv.service-ethernet-mainInterfaceName
           description $descr
         exit
```

To use global variables to create CLI templates:

Step 1 Choose **Configuration** > **Templates** > **Global Variables** to create new global variables.

To use existing global variables that are pre-populated in Cisco EPN Manager for each service type (CE, L3VPN, and CEM), skip to Step 4.

Step 2 Click the Add '+' icon. To edit existing variables, select the global variable and click the Edit button.

Step 3 Specify the following parameters and click **Save**. Your changes are saved in the Cisco EPN Manager database and are not immediately deployed to the device.

- **Name**: Enter a unique name for the variable ensuring that the name starts with the letters 'gv' followed by the type of service this global variable is relevant to. You can use special characters such as the dot, hyphen, and underscore.
- **Description**: Enter a unique description for easy identification of the variable. This description is extremely important to help identify the purpose of this variable that may be used in CLI templates. The CLI templates could further be used to provision services (such as L2 and L3 services). And on the service creation page, you will rely completely on the variable description to identify the purpose of the variable.
- **Type**: Use one of the following options to specify the type of variable:
  - **String**: Enables you to create a text box for CLI templates. Only the string type of variable is applicable to CLI templates used in service provisioning.
  - **Integer**: Enables you to create a text box that accepts only numeric value. It can later be configured to specify a range for the value.
  - **IPv4 Address**: Enables you to create a text box that accepts only IPv4 addresses for CLI templates.
  - **Drop-down**: Enables you to create a drop-down list for CLI templates.
  - **Check box**: Enables you to create a check box field for CLI templates.
  - **Radio Button**: Enables you to create a radio button for CLI templates.
  - **Text Area**: Enables you to create a text area which allows multiline values for CLI templates.
- **Value**: Specify the values that must be generated based on the selected Type values explained above.

  If you want to specify the value during service creation or during CLI template creation, you can choose 'Not Available' as a place holder.
- **Display Label**: Enter how you want the variable to be displayed in the Cisco EPN Manager GUI.

Step 4 Associate the global variable with a CLI template:

a) Navigate to **Configuration > Templates > Features & Technologies**.

b) To create a new CLI template from scratch, see Create a New CLI Configuration Template Using a Blank Template, on page 454.

c) To associate global variables with existing templates, see Create a New CLI Configuration Template Using An Existing Template, on page 455.

d) To add global variables, from the Template Details section, use the **Add Global Variable** search field to locate the global variable. For easy identification, you can also use the **Global Variable** hyperlink displayed at the top right corner of the page. You can use global variables along with CLI, and/or template variables in the same CLI template.

You can identify the services that the variables belong to by looking at the variable name. Variables applicable to CE services, have variable names that start with the letters 'gv.ce-service-ethernet*'. Variables applicable to L3VPN services, have variable names that start with the letters 'gv.l3vpn-service-l3vpn*'. These variables can be associated with new or existing CLI templates.

a) Make the required changes to the CLI template and click **Save as New Template**.
b) The CLI template is now saved and displayed under **My Templates > CLI Templates (User Defined)**.
c) (Optional) Deploy the CLI template to the devices as explained in Deploy Templates to Devices, on page 466.

Step 5 (Optional) To provision services (L2, L3VPN, CEM, Flex LSP, Layer 3 link) using CLI templates (associated with global and template variables), see, Extend a Circuit/VC Using Templates, on page 609.

Example

Sample Global Variables Available in Cisco EPN Manager:

- Following are the sample global variables that can be used with L3VPN services:

☐	gv.service-l3vpn-InterfaceDetailsMap	Interface Detail	String
☐	gv.service-l3vpn-bgpASNumber	BGP AS Number	String
☐	gv.service-l3vpn-bgpNeighborASNu...	BGP Neighbor AS Number	String
☐	gv.service-l3vpn-bgpNeighborAddres...	Neighbor Address Family	String
☐	gv.service-l3vpn-bgpNeighborsList	BGP Neighbor	String
☐	gv.service-l3vpn-bgpRouterId	BGP Router ID	String
☐	gv.service-l3vpn-bridgeDomainList	Bridge Domain ID	String
☐	gv.service-l3vpn-mainInterfaceName...	Main Interface Name	String
☐	gv.service-l3vpn-ospfArea	OSPF Area	String
☐	gv.service-l3vpn-ospfProcessId	OSPF Process ID	String
☐	gv.service-l3vpn-serviceInstanceNu...	Service Instance Number	String
☐	gv.service-l3vpn-serviceInterfaceNa...	Sub-Interface or BDI/BVI Name	String
☐	gv.service-l3vpn-vrfAddressFamilyList	VRF Routing Address Family	String
☐	gv.service-l3vpn-vrfName	VRF Name	String

- Following are the sample global variables that can be used with CEM services:

gv.service-cem-auNumber	AU (AU-3 or AU-4) number	String
gv.service-cem-cemFrameType	CEM frame type	String
gv.service-cem-cemGroupNumber	CEM group number	String
gv.service-cem-cemGroupNumberList	CEM group number list for local connects	String
gv.service-cem-cemInterfaceName	CEM interface name	String
gv.service-cem-cemInterfaceNameList	CEM interface name list for local connects	String
gv.service-cem-controllerInterfaceName	Controller name	String
gv.service-cem-e1Number	E1 number	String
gv.service-cem-l2vpnContextName	L2VPN context name	String

Import and Export a CLI Configuration Template

These topics explain how to export and import configuration templates. Templates can be exported templates have an .xml file name; multiple templates are exported as a zip file.

- If you export multiple configuration templates, the .xml files are placed in a zip file with the prefix name **Exported Templates**.
- Single files are exported and imported as .xml files
- You can import multiple .xml files by selecting individual files or by importing a zip file.
- When you import CLI templates, the user-defined global variables that are part of the file are not imported automatically. You need to add these variables to the CLI template manually.
- When you import CLI templates using CLI commands, ensure to use the variable names with valid syntax. The variable name should start with alphabets or an underscore (_). Supported special characters are underscore and hyphen.

Warning Template variables will not be validated during import, so ensure to use the proper variable names.

Step 1 Choose **Configuration > Templates > Features & Technologies.** .

Step 2 To export a configuration template:

a) Select the template(s) that you want to export and click .
b) Save the files at the desired location.

Note Template export fails if there are XML specific special characters in the **Description** or **Template Detail** fields.

Step 3 To import a configuration template:

a) Under the **CLI Templates** folder, hover your mouse cursor over the "i" next to **CLI**.

b) Click **Show All Templates**, then click **Import**.
c) In the **Import Templates** dialog box, choose the **My Templates** folder where you want to import the templates, then click **Select Templates** and navigate to the file you want to import.
d) Confirm your choices, then click **OK**.

Create a New Composite Template

All out-of-the-box and user-created templates can be added to a single composite template, which aggregates all of the individual feature templates that you need. When you create a composite template, you can also specify the order in which member templates should be executed. You can use composite templates to make changes to single or groups of devices.

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.
Step 2 Expand the **Composite Templates** folder and choose **Composite Templates**.
Step 3 In the **Template Basic** area, enter a name for the template.
Step 4 In the **Template Detail** area, choose the templates to include in the composite template. Using the arrows, place the templates in the in the order in which they should be deployed to the devices. For example, to create an ACL and associate it with an interface, put the ACL template first, followed by the interface template.
Step 5 Click **Save as New Template**. After you save the template, and apply it to your devices (see Deployment Flow for Composite Templates Using the Wizard).

Create a Shortcut to Your Templates Using Tags

When you apply a tag to a template, the template is listed under the **My Tags** folder. Tagging a configuration template helps you:

- Search a template using the tag name in the search field
- Use the tagged template as a reference to configure more devices

To tag an existing template, follow these steps:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.
Step 2 Expand the **My Templates** folder and choose the template that you want to tag.
Step 3 Enter a tag name in the **Tag as** text box, then click **Save**.

Create a Troubleshooting Template

Use troubleshooting templates to define a set of reusable non-configuration commands (for example "show" command) to run on the devices.

To create a Troubleshooting template:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**.

Step 2 Expand **CLI Templates**, then choose **CLI**.

Step 3 In the **Template Basic** area:

a) Enter a name for the template.

b) Select the **Troubleshooting Template** checkbox. Doing this will change the template to a troubleshooting template and tag it as a troubleshooting template.

Note

a. You can create troubleshooting templates only of type devices.

b. Do not edit the 'TroubleshootingTemplate' tag in the **Tags** field.

Step 4 Specify the commands and variables as required in the **Template Detail** area. For information about creating variables, see Entering Variables in a Template, on page 456.

Step 5 Save your template. Click **Save as New Template**, specify the folder (in **My Templates**) in which you want to save the template, then click **Save**.

Note "MODE_ENABLE" cannot be used with Troubleshooting templates.

What to do next

The procedure to deploy the troubleshooting template and edit/retry a failed template deployment is similar to that in case of CLI templates. Refer to the following sections:

- Deployment Flow for CLI Templates using the Wizard, on page 469
- Edit and Retry a Failed Template Deployment, on page 475

Deploy Templates to Devices

These topics describe the ways you can deploy (run) groups of commands on devices using configuration templates:

- Create Configuration Groups for Deploying Templates to Groups of Devices
- Deployment Flow for Configuration Group Using the Wizard
- Deployment Flow for CLI Templates using the Wizard

- Deployment Flow for Composite Templates Using the Wizard
- Deploy Templates to Devices Without Using Configuration Groups

Control Configuration Deployment Behavior

As an administrator, you can choose to have device configurations backed up or rolled back when users deploy new device configuration templates.

Archive Device Configurations Before Template Deployment

Cisco EPN Manager automatically backs up all device running and startup/admin configurations before deploying new configuration templates if the **Backup Device Configuration** setting is enabled.

1. Choose **Administration** > **Settings** > **System Settings** > **Inventory** > **Configuration**.
2. Select the **Backup Device Configuration** check box.
3. Click **Save**.

Roll Back Device Configurations on Template Deployment Failure

Cisco EPN Manager automatically rolls back each device to its last archived running and startup/admin configurations when any attempt to deploy a new configuration template to the device has failed.

1. Choose **Administration** > **Settings** > **System Settings** > **Inventory** > **Configuration**.
2. Select the **Rollback Configuration** check box.
3. Click **Save**.

Create Configuration Groups for Deploying Templates to Groups of Devices

If you have devices that require the same configuration, you can create a *configuration group* that contains devices and templates that can be applied to those devices. Creating a configuration group allows you to quickly apply new templates without remembering to which devices the new templates should be deployed.

Composite templates allow you to group smaller templates together, but configuration groups specify the *relationship* between the templates and the groups of devices, and the order in which commands are executed.

Step 1 Choose **Configuration** > **Templates** > **Configuration Groups**.

Step 2 In the Configuration Group Basic area, enter a name.

Step 3 To display devices from which you can make selections, in the Template Selection area, add one or more templates by clicking **Add** and selecting the templates. This also populates the Device Type field.

Step 4 Add additional templates by clicking **Add** in the Template Selection area. You cannot choose templates that are mutually-exclusive; for example, you cannot choose Add-Host-Name-IOS and Add-Host-Name-IOS-XR.

Step 5 Select the devices on which you want to deploy the template, then click **Next** to choose the input option.

Step 6 In the Device Selection area, select the devices you want to add to the configuration group.

Step 7 If you have multiple templates, the order in which templates will be listed by selecting one and clicking the up or down arrow.

Step 8 Click **Save as New Configuration Group**.

Deployment Flow for Configuration Group Using the Wizard

Note This deployment flow is not applicable for Controller based templates.

Step 1 After you create a configuration group, click **Deploy**. The **Template Deployment -Prepare and Schedule** wizard page opens.

Step 2 In the **Templates** area, view the templates that are added in the configuration group.

Step 3 In the **Deployed on Devices** area and during creation of Configuration Group, view the devices that you have chosen during creation of configuration group.

Step 4 In the **Value Assignment** area, from the **Select Template** drop-down list, choose a CLI template and an appropriate device. You can view the device details on which the template is going to be deployed, CLI Preview details, and so on. Click **Apply**.

Step 5 (Optional) Schedule the deployment job in the **Schedule** area:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

  Failure Policy:

  - **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  - **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
  - **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
  - **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 6 In the **Summary** area, view the summary of the deployment.

Step 7 Click **OK** to deploy the template.

Step 8 Click **Job Status** in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Deployment Flow for CLI Templates using the Wizard

Step 1 After creating the CLI template, click **Deploy**. The Deployment Wizard page opens.

Step 2 Select the devices on which you want to deploy the template, then click **Next** to choose the input option.

Step 3 Select the devices on which you want to deploy the template from the **Add devices** table. The selected devices appear in the **Devices to deploy** table.

Step 4 Select the mode in which you want to deploy the template. The options are **Work Flow** and **Export/Import CSV**.

Step 5 Click the **Work Flow** option and click **Next**. See *Step 6* .

Step 6 Alternately, click **Export/Import CSV** option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.

a) Uncheck the **Do you want Optional Parameters** check box, if you want to skip the optional fields while filling the configuration values in the CSV file.
b) Click **Export CSV** to download the CSV template to your local system.
c) Enter the configuration values for each specific device in the downloaded CSV template.
d) Click **Import CSV** to upload the updated CSV file. The input values automatically get updated.
e) Click **Next** to input values.

Step 7 In the **Input Values** tab, you can toggle between **Form** and **CLI** view. Configure the following in the Input Values tab:

a) Enter all the mandatory fields for each template, then click **Apply**.

Note For profile management, Fault-Profile-Definition and Fault-Profile-Apply templates are available. While deploying these templates, in the Input Values window you must enter the applicable fault tags for the selected fault type from the reference table.

If the validation is successful, then the border of the circle around the selected template changes to green.

Note The successful validation message means that the change has been applied only to the selected devices in the workflow. To complete the configuration, perform the remaining steps in the procedure.

Step 8 After entering the necessary configuration values, click **Next** or **CLI** to confirm the device and template configuration values.

Step 9 Schedule the deployment job using **Schedule Deployment** tab, if necessary:

- Create a meaningful deployment job name, then specify whether to run now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly, or yearly basis.
- You can configure the following job options:

  Failure Policy:

  - **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
  - **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices that are chosen for deployment will be same as the device order in Value assignment pane.

- **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
- **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 10 Click **Next** to view the job deployment summary.

Step 11 On the **Deployment Summary** tab, you can see the CLI view o each device.

Step 12 Click **Finish** to deploy the template.

Step 13 Click **Job Status** in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Note The SG220 device does not support any of the configuration template deployments whereas the SG300 and SG500 devices support CLI template deployment. However, both the SG300 and SG500 devices support only the following system CLI templates.

- APIC Bootstrap
- Banner Configuration-IOS
- Best_Practice_Access_3k
- Best_Practice_Access_4k
- Best_Practice_Global
- Certificate Authority-IOS
- Configure SNMPv3
- Configure VLAN
- Configure_Access_Port
- Crypto Map Configuration
- DNS Configuration
- EEM Environmental Variables
- Enable Password-IOS
- EtherChannel
- HTTP SWIM Image Upgrade Template
- HTTP-HTTPS Server and WSMA Configuration-IOS
- Local Management User
- Plug And Play Bootstrap
- RADIUS_AUTH
- Radius Acct. Servers
- Radius Configuration-IOS
- Reload Configuration-IOS
- TACACS Server
- TACACS-POST-PNP
- Trap Receiver
- stp

Note You can also push a template-based configuration (user-defined template or system-defined template) to devices by choosing **Inventory** > **Device Management** > **Configuration Archive** > **Devices/Archives** > **Deploy Config**.

Deployment Flow for Composite Templates Using the Wizard

Step 1 Choose **Configuration > Templates > Features & Technologies > Composite Templates > Composite Templates**.

Step 2 Enter the required information in the Template Basic section.

Step 3 In the Template Detail section, choose the templates to include in the composite template, and click **Save as New Template**.

Step 4 After creating the composite template, click **Deploy**. The Deployment wizard page opens.

Step 5 Select the devices on which you want to deploy the template.

Step 6 Select the devices on which you want to deploy the template from the **Add devices** table. The selected devices appear in the **Devices to deploy** table.

Step 7 Select the mode in which you want to deploy the template. The options are **Work Flow** and **Export/Import CSV**.

Step 8 Click the **Work Flow** option and click **Next**. See *Step 6*.

Step 9 Alternately, click **Export/Import CSV** option, to update all the template properties for the selected devices using the CSV Export/Import mechanism.

a) Uncheck the **Do you want Optional Parameters** check box, if you want to skip the optional fields while filling the configuration values in the CSV file.
b) Click **Export CSV** to download the CSV template to your local system.
c) Enter the configuration values for each specific device in the downloaded CSV template.
d) Click **Import CSV** to upload the updated CSV file.The input values automatically gets updated.
e) Click **Next** to input values.

Step 10 In the **Input Values** tab, you can toggle between **Form** and **CLI** view. Configure the following in the Input Values tab:

a) Select templates for a device from the navigation widget. To select templates, click the circle (T1, T2, T3, T4, T5 ...) in the upper right corner. If there are more than five templates, click three dots. The drop-down list will pop-up with all the available templates.
b) Enter all the mandatory fields for each template, then click **Apply**.

If the validation is successful, then the border of the circle around the selected template changes to green and green tick mark appears adjacent to the selected templates for the available templates in the popup.

Step 11 After entering the necessary configuration values, click **Next** or **CLI** to confirm the device and template configuration values.

Step 12 Schedule the deployment job using **Schedule Deployment** tab, if required:

- Create a meaningful deployment job name, then specify whether to run the now or in the future.
- You can also schedule the job to run periodically on hourly, daily, weekly, monthly or yearly basis.
- You can configure the following job options:

  Failure Policy:

- **Ignore failure and continue**—This is the default option. The devices are randomly picked up for template deployment. If the job fails on a device, the job skips the device and continues with the remaining devices. The Job results show success/failure information for all the selected devices.
- **Stop on failure**—If the job fails to execute on a device, the job is stopped. The job results are updated only for the devices on which the job was executed successfully and for other devices which didn't undergo template deployment, "Not Attempted" message is shown. The order of devices chosen for deployment will be same as the device order in Value assignment pane.
- **Copy Running Config to Startup**—If the template deployment job succeeds, the running configuration of the device is copied to startup configuration.
- **Archive Config after deploy**—Creates a new config archive job and archives the configuration of devices after successfully deploying the template.

Step 13 Click **Next** to view the job deployment summary.

Step 14 On the **Deployment Summary** tab, you will see the CLI view for each of the device.

Step 15 Click **Finish** to deploy the template.

Step 16 Click **Job Status** in the pop-up dialog box to launch the Job Dashboard to view the status of the job.

Deploy Templates to Devices Without Using Configuration Groups

Once a template is saved, it can be deployed (run on) devices. You can deploy a template from the **Configuration** > **Templates** > **Features & Technologies** navigation area, or by using Configuration Groups, which is launched from **Configuration** > **Templates** > **Configuration Groups** (see Create Configuration Groups for Deploying Templates to Groups of Devices , on page 467).

To deploy a customized or system template from the **Features & Technologies** navigation area:

Step 1 Choose **Configuration** > **Templates** > **Features & Technologies**

Step 2 Expand the drawer that contains the template(s) you want to deploy.

Step 3 Choose the templates you want to deploy, and click **Deploy**.

Step 4 In the **Template Deployment** window, check the settings and schedule and click **OK**.

Role-Based Access Control for Template Deployment

Cisco EPN Manager supports role-based restrictions for template deployment. With this feature, you can allow users from an authorized user group to only view and deploy a template. All other operations on the template such as Create, Edit, Delete, Import, and Export are restricted.

Note This feature is applicable only for CLI templates.

Task and job permissions

Log in as an admin or root user to create user groups with the following task permissions. (Task permissions are located in the **Administration** > **Users** > **Users and Roles** > **Users** window.)

- Enable **Deploy Configuring Access**
- Disable **Design Configuration Template Access**

Enable the following job permissions for the user group to manage the config deploy job. Without these job permissions, users cannot view, edit, or run the job.

- Edit Job
- Run Job
- View Job

Enable role-based access for template deployment

To enable role-based access control for template deployment, login as a Root, Admin, or Config user and assign the template to a user group from the **User group** drop-down list in the **Template Basic** area (**Configuration** > **Templates** > **Features & Technologies** > **CLI Templates** > **CLI**). The **User group** drop-down list contains only those user groups that have been configured with task permissions mentioned earlier. You can assign the template to one or more user groups from this list.

After you have assigned the template to a user group, only users from the authorized user group can view and deploy the template. Users from unauthorized user groups cannot view the template.

For a composite template, only users with appropriate user group permissions to execute all the included CLI Templates are allowed to deploy the template.

Deploy users can edit or run the job only for the templates that are assigned to the associated user group.

Note

- Templates that are not assigned to any user group can be accessed and deployed by all users.
- When importing templates associated with user group(s), ensure that the deploy ‘user group’ roles are same between source and destination system for the RBAC template to work seamlessly.
- In case of any mismatch in the deploy user group roles, it is recommended that you reassign the template to the user group OR edit the template to remove all existing user group(s) associations and save the template.

Check the Status and Results of a Deployed Configuration Template

When you deploy a configuration template, Cisco EPN Manager displays a dialog box with a hyperlink that directs you to the Jobs window. From here you can:

- View the results of the command by clicking the History tab and expanding the job instance.

- Repeat the deployment, or schedule it for a later time
- Manage the job (delete it, pause it, resume it, and so forth).

Template Deployment Failure Syslog

When a template deployment to the device fails, Cisco EPN Manager generates a syslog with severity ERROR and sends it to the destination IP that is configured in EPNM.

To configure this destination IP, see Forward System Audit Logs As Syslogs, on page 867 for more information.

To enable the generation of syslogs:

1. Navigate to **Administration** > **Settings** > **Logging** > **Syslog Settings**.
2. Select the **Enable Syslog** checkbox.
3. Click **Save**.

Edit and Retry a Failed Template Deployment

A template deployment may fail on device(s) partially or completely due to incorrect or invalid values provided during deployment.

The Edit and Retry functionality helps to reexecute such failed jobs by modifying the previously provided inputs.

Important You can use the Edit and Retry functionality to reexecute failed jobs in case of CLI templates, Troubleshooting templates and Composite Templates.

You can view the status of the job in Job Dashboard. The Edit icon () will be enabled on the failed configuration template jobs. On clicking this icon, the **Template Deployment - Edit and Retry** window opens, which helps you to correct previously provided input(s) and retry the deployment.

The template deployment may fail due to any of the following reasons:

1. Incorrect/unsupported values provided for variables:
   a. Choose **Administration** > **Dashboards** > **Job Dashboard**.
   b. Select the failed deployment job in the Jobs page.
   c. Click the Edit icon. Edit the values as required in the **Template Deployment - Edit and Retry** window, and then click **OK**.
2. One or more device(s) unreachable/wrong credentials:
   a. Fix the device reachability issues.
   b. Choose **Administration** > **Dashboards** > **Job Dashboard**.
   c. Select the failed deployment job in the Jobs page.

d. Click **Run** in the Jobs page to rerun the deployment.

3. Incorrect/invalid commands in configuration templates:

This requires modification of the template. You cannot use the Edit and Retry functionality in this case.

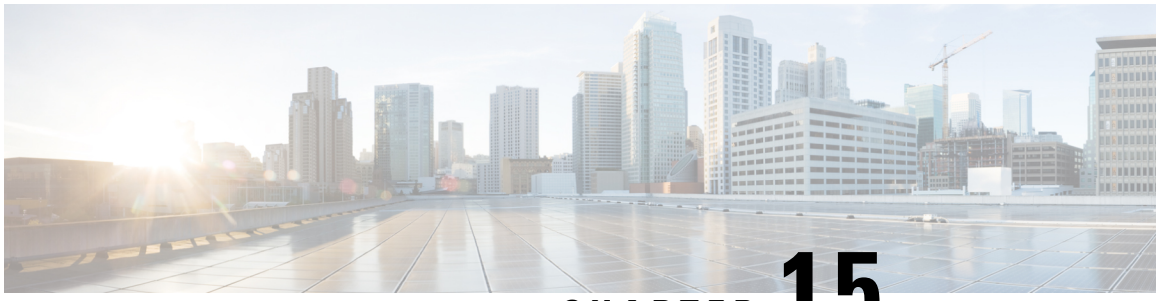
If you modify the original template, edit and retry for the failed configuration template job will be blocked. For modified templates, you should deploy the templates using the Deployment wizard.

Note

- Edit and retry operation is not supported for configuration groups, and templates of type Ports.
- If you are upgrading the Cisco EPN Manager version, you must clear the browser cache before attempting this operation.

PART VI

Manage Circuits



CHAPTER 15

Overview of Circuit/VC Discovery and Provisioning

Circuits/VCs Provisioning Overview

Cisco EPN Manager supports provisioning of circuits/VCs for various technologies such as Carrier Ethernet (CE), Optical/DWDM, L3VPN, Circuit Emulation, Segment Routing, and MPLS Traffic Engineering. Mostly, a circuit spans across multiple devices. You must make configuration changes across multiple devices to provision a circuit. Cisco EPN Manager provides a Provisioning Wizard that allows you to make the required configuration changes across multiple devices that participate in a circuit.

The Provisioning Wizard collects all the required information in a step-by-step approach and generates the required configuration for all the devices. You can review the configurations generated for each device, and then choose to either make any changes in the service parameters or deploy the configurations to the devices.

The configuration changes are deployed to the participating devices as an 'atomic' transaction. Cisco EPN Manager does a best-effort attempt to either carry out all these operations together or does none at all. To implement the concept of 'atomic' transaction, Cisco EPN Manager has the rollback feature, which helps to recover from failures during provisioning.

When configuring multiple devices, if the configuration fails in any of the devices, Cisco EPN Manager does a best-effort to rollback the configuration changes made so far in all the participating devices. The device configuration states are restored to the same state, which was there before the provisioning operation was attempted.

Note Cisco EPN Manager does not support services with endpoints on main interfaces; only services with endpoints on sub-interfaces are supported.

For L3VPN services, Cisco EPN Manager supports discovery but not provisioning on main interfaces. For L2VPN services, neither discovery nor provisioning is supported on main interfaces.

Supported Carrier Ethernet VCs

In a Carrier Ethernet (CE) network, data is transported across point-to-point and multipoint-to-multipoint Ethernet Virtual Connections (EVCs) and Operator Virtual Connections (OVCs) according to the attributes and definitions of the various service types—that is, E-Line, E-LAN, E-Tree, E-Access, and EVPN Virtual Private Wire Service.

Each EVC type has a port-based service and a VLAN-based service. These are differentiated by the method for service identification used at the UNIs. EVCs using all to one bundling UNIs (port-based) are referred to as 'Private', while EVCs using UNIs that are service multiplexed (VLAN-based), are referred to as 'Virtual Private'

For E-Line, E-LAN, and E-Tree services, each EVC carries data in the form of CE service frames from UNI (User Network Interface) to UNI, where the UNI is the physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber. E-Access Operator Virtual Circuits (OVCs) allow service provider interconnections at the ENNI (External Network Network Interface), which is the physical demarcation point between the responsibility of two interconnecting Service Providers.

Each EVC can be configured with a rich set of attributes that include bandwidth profiles (Committed Information Rate - CIR, Excess Information Rate - EIR, Committed Burst Size - CBS, Excess Burst Size - EBS), multiple classes of service, application-oriented performance objectives, traffic management, forwarding rules, and so on.

Cisco EPN Manager supports the discovery and provisioning of the following EVC types, which are described in these topics:

- E-Line, on page 481:
  - MPLS to the edge
  - Single-segment pseudowire
  - Ethernet access—local, G.8032, ICCP-SM
- E-LAN, on page 482
  - MPLS to the edge
  - Single-segment pseudowire
  - VPLS/H-VPLS with redundant pseudowire
  - Ethernet access—VPLS-based
- E-Tree, on page 483—MPLS to the edge
- E-Access, on page 483—MPLS to the edge

• EVPN Virtual Private Wire Service (VPWS), on page 484
• Multisegment Pseudowire, on page 484

Core Technology for Multipoint EVCs

The core technology for the E-LAN or E-Tree EVC can be either VPLS (Virtual Private LAN Services) or H-VPLS (Hierarchical VPLS).

- VPLS—A Layer 2 VPN technology that provides Ethernet-based multipoint-to-multipoint communication over MPLS networks. VPLS allows geographically dispersed sites to share an Ethernet broadcast domain by connecting sites through pseudowires. The network emulates a LAN switch or bridge by connecting customer LAN segments to create a single bridged Ethernet LAN.
- H-VPLS— Partitions the network into several edge domains that are interconnected using an MPLS core. The edge devices learn only of their local U-PE devices and therefore do not need large routing table support. The H-VPLS architecture provides a flexible architectural model that enables Ethernet multipoint and point-to-point Layer 2 VPN services, as well as Ethernet access to Layer3 VPN services, enabling service providers to offer multiple services across a single high-speed architecture.

In E-TREE EVCs, H-VPLS supports redundancy. Two hubs operate as connectors through which all traffic passes. If the primary hub fails, traffic is switched to the backup hub. With H-VPLS as the core technology, there is no direct connection between the E-tree root and leaf. H-VPLS is used together with split-horizon capabilities to prevent leaf to leaf communication.

If VPLS is used as the core technology, redundancy is not supported and there is a direct connection between root and leaves. The hub is located in the root, meaning that the root assumes the role of the hub.

E-Line

E-Line refers to an Ethernet service that is based on a point-to-point EVC. There are two types of E-Line VCs:

- Ethernet Private Line (EPL), which has the following characteristics:
  - Port-based
  - Uses a point-to-point EVC between two UNIs to provide a high degree of transparency such that service frames, headers, and most Layer 2 protocols are identical at the source and destination UNI.
  - All to one bundling where all CE-VLAN IDs are bundled to one EVC. No service multiplexing.

Note The L2VPN services are discovered only if they are configured on sub interfaces or service instances, and are not supported on main-interfaces.

- Ethernet Virtual Private Line (EVPL), which has the following characteristics:
  - VLAN-based
  - Uses a point-to-point EVC between two UNIs, but does not provide full transparency as EPL, that is, all Layer 2 control protocols are discarded at the UNI.
  - Allows service multiplexing, which means that more than one EVCs can be supported at UNI.

Following are the limitations of E-Line services:

- Assignment of a MEP group for E-line services after promotion may not match the scenario seen during service creation.
- MEP group for an E-line service is assigned based on lexicographical order of the device name.
- XConnect must be up before registering to CFM. It is a device behavior. CFM details are shown in view 360 for DOWN service only if PW or neighbor is already established.
- If a Pseudowire ID has already been assigned to a service, it cannot be reused even if that service is no longer active. To reuse an already assigned Pseudowire ID, you must manually reset the inuse flag to 0 for that ID in the 'numberresourcepoolallocation' table. The steps to do so are as follows:
  - Initiate an SSH connection to Cisco EPN Manager as a *root* user.
  - In the following file, replace <value> with the required number to make the EPL available for use:

    sh /opt/CSCOlumos/bin/sql_execution.sh "update numberresourcepoolallocation set inuse=0 where value=<value>"

E-LAN

E-LAN refers to an Ethernet service that is based on a multipoint-to-multipoint EVC. There are two types of E-LAN VCs:

- Ethernet Private LAN (EP-LAN), which has the following characteristics:
  - Port-based
  - All-to-one bundling at UNI
  - Transparent, no manipulation of CE-VLAN IDs and PCP bits
  - EP-LAN multiport transparency is more complex than EPL

Note The L2VPN services are discovered only if they are configured on sub interfaces or service instances, and are not supported on main-interfaces.

- Ethernet Virtual Private LAN (EVP-LAN), which has the following characteristics:
  - VLAN-based
  - Allows service multiplexing and bundling

Following are the limitations of E-LAN services:

- For XR devices, probe name must have a unique probe id – PM2_<probeid>_*.
- MEP group must be provided even if CFM is disabled for the services (ELAN/ETREE) during promotion.
- **`localhost`** and **`hairpin`** are not supported for E-LAN.

E-Tree

An E-Tree VC is a rooted multipoint VC that connects a number of UNIs providing sites with hub and spoke multipoint connectivity. Each UNI is designated as either *root* or *leaf* . A root UNI can communicate with any leaf UNI. A leaf UNI can communicate only with a root UNI, not with another leaf UNI.

E-Tree VCs provide the separation between UNIs required to deliver a single service instance in which different customers (each having a leaf UNI) connect to an ISP which has one or more root UNIs. Having more than one root UNI is useful for load sharing and resiliency schemes.

There are two types of E-Tree VCs:

- Ethernet Private TREE (EP-TREE), which has the following characteristics:
  - Rooted multipoint, port-based.
  - All-to-one bundling at the UNI.
  - Simpler than typical hub and spoke configuration using multiple EPLs. Hub function is performed by the root UNI.
  - Provides CE-VLAN tag preservation and tunneling of key Layer 2 Control Protocols.
  - Supports CE-VLAN CoS preservation.
- Ethernet Virtual Private TREE (EVP-TREE), which has the following characteristics:
  - Rooted multipoint, VLAN-based.
  - Provides an alternative to multiple EVPLs multiplexed at the hub site.
  - Used in cases where one or more of the subscriber's UNIs also supports other services, e.g., EVPL or EVP-LAN.

Following is the limitation of E-Tree services:

- **`localhost`** and **`hairpin`** is not supported for E-Tree.

E-Access

An Ethernet Access service allows a service provider to construct an Operator Virtual Connection (OVC) between two customer sites where one of the sites is located outside of the service provider's own network. In such cases a service provider uses an E-Access service offered by a local wholesale access provider to reach the out-of-franchise UNI. The service provider connects to the E-Access service at an ENNI, and traffic is forwarded between the ENNI and the out-of-franchise UNI across an Operator Virtual Connection (OVC).

E-Access definitions include attributes related to the external interfaces, in this case, the ENNI and the UNI, as well as attributes related to the virtual Ethernet connection associating these external interfaces. E-Access services use a point-to-point OVC to associate one OVC endpoint at an ENNI and one OVC endpoint at a UNI.

There are two types of E-Access VCs:

- Access EPL, which has the following characteristics:
  - Private or port-based
  - One OVC per UNI
  - All CE-VLAN IDs are mapped to the OVC
- Access EVPL, which has the following characteristics:

- VLAN-based
- Can be multiple OVCs per UNI
- Multiple but not all CE-VLAN IDs are bundled to one OVC

EVPN Virtual Private Wire Service (VPWS)

The EVPN-VPWS is a BGP control plane solution for point-to-point services. It implements the signaling and encapsulation techniques for establishing an EVPN instance between a pair of PEs. It has the ability to forward traffic from one network to another without MAC lookup. The use of EVPN for VPWS eliminates the need for signaling single-segment and multi-segment PWs for point-to-point Ethernet services. The EVPN-VPWS technology works on IP / MPLS core; IP core to support BGP and MPLS core for switching packets between the endpoints.

Multisegment Pseudowire

Cisco EPN Manager supports discovery of point-to-point EPL and EVPL services which use multisegment pseudowire.

When you configure your device for a multisegment pseudowire based service, Cisco EPN Manager discovers all the pseudowire segments that are part of the configuration as one service.

After you have configured your device for this service, you can view the edge endpoints of a multisegment pseudowire under Endpoints in the **Circuit 360 view** of the Cisco EPN Manager. The **Overlay** and **Multilayer Trace** tabs of Cisco EPN Manager display all the NEs participating in the multisegment pseudowire; including head, mid, and tail. In addition, these tabs also display the underlying SR policies and MPLS tunnels that are configured and traversed by each pseudowire segment. Make sure that you have the following device configurations before you set up a multisegment Pseudowire service:

- To Enable GI

```
logging <Server_IP> vrf default severity info port default
logging hostnameprefix <Server_IP>
snmp-server host <Server_IP> traps vrf
snmp-server host <Server_IP> traps version 2c public
```

- To Support Interface up/down via GI

```
snmp-server traps l2tun sessions
snmp-server traps l2tun tunnel-up
snmp-server traps l2tun tunnel-down
snmp-server traps l2tun pseudowire status
```

Note

- Multisegment pseudowire supports discovery of EVPL and EPL services on all IOS XR devices. Provisioning is not supported.
- As this is only for service discovery, promotion is disabled for services with multisegment pseudowire configurations.
- When you associate a multisegment pseudowire with Multi Service Protection (MSP) over a preferred path of MPLS-TE tunnel or SR-TE, the associated Y.1731 and Y.1564 protocols are not supported. You can however use Y.1731 and Y.1564 services over MSP when a preferred path is not specified on the multisegment pseudowire.

EVPN ELAN Visualization

EPNM supports EVPN ELAN Single Homing (from RFC 7432) network management comprising of XE and XR platforms. EVPN ELAN Visualization is supported only for discovery and not for provisioning and promotion.

Supported Network Structure for Provisioning EVCs

Cisco EPN Manager can provision EVCs and OVCs over a mix of access networks. The endpoints can be configured directly on an MPLS router, an Ethernet Access switch, or an nV satellite attached to a Cisco ASR 9000 router. The EVCs may have endpoints in different Ethernet Access networks, in the same network, or on the same device. Cisco EPN Manager will configure as much as is needed to create the connectivity.

EVCs can be provisioned over the following networks:

- MPLS Domain—Cisco EPN Manager assumes that the managed network contains a single MPLS domain. Any router can communicate with any other router via a targeted LDP session. Alternatively MPLS end-to-end connectivity can be achieved using MPLS Traffic Engineering or segment routing.
- Ethernet Access Network—Cisco EPN Manager supports EVC provisioning over Ethernet Access networks attached to a central MPLS domain. The networks are discovered by the system. EVCs can be provisioned over a G.8032 access ring or over ICCP-SM links. The access network can be:
  - A G.8032 ring. This should include a router to enable the creation of EVCs that cross the MPLS domain.
  - A G.8032 open ring, which means a sequence of links.
- Cisco ASR 9000 nV Satellite Topology—Cisco EPN Manager can configure EVCs on single-homed nV satellite devices attached to an Cisco ASR 9000 host.

To support service discovery and provisioning, Cisco EPN Manager must discover the topology in the access network. For successful discovery, the following prerequisites must be fulfilled:

- For ICCP-SM, LAG must be configured with LACP.
- For G.8032, CDP or LLDP must be configured on the ring ports.

Supported Optical Circuits

A circuit represents an end-to-end connection between two or more connection termination points (CTPs). A circuit consists of an alternating series of cross-connections and link connections. In its simplest form, a circuit consists of a single cross-connection (if the circuit is defined between two CTPs on the same NE). A circuit can be bidirectional or unidirectional, point-to-point or point-to-multipoint, and protected or unprotected.

Cisco EPN Manager supports the provisioning of Dense Wavelength Division Multiplexing (DWDM) optical channel (OCH) circuit types and Optical Transport Network (OTN) circuit types. The DWDM optical technology is used to increase bandwidth over existing fiber optic backbones. It combines and transmits multiple signals simultaneously at different wavelengths on the same fiber. In effect, one fiber is transformed into multiple virtual fibers.

Cisco EPN Manager supports the following optical circuits types:

- Dense Wavelength Division Multiplexing (DWDM) Circuits, on page 486
  - Optical Channel Network Connection (OCHNC) WSON, on page 486

Dense Wavelength Division Multiplexing (DWDM) Circuits

The following topics describe the different optical channel (OCH) and media channel (MCH) circuit types.

Optical Channel Network Connection (OCHNC) WSON

OCHNC WSON circuits establish connectivity between two optical nodes on a specified C-band wavelength. The connection is made through the ports present on the wavelength selective switches, multiplexers, demultiplexer, and add/drop cards. In an OCHNC WSON circuit, the wavelength from a source OCH port ingresses to a DWDM system and then egresses from the DWDM system to the destination OCH port.

Optical Channel Client Connection (OCHCC) WSON

OCHCC WSON circuits extend the OCHNC WSON to create an optical connection from the source client port to the destination client port of the TXP/MXP cards. An OCHCC WSON circuit represents the actual end-to-end client service passing through the DWDM system. Each OCHCC WSON circuit is associated to a pair of client or trunk ports on the transponder (TXP), muxponder (MXP), GE_XP (in layer-1 DWDM mode), 10GE_XP (in layer-1 DWDM mode), or ITU-T line card. The OCHCC WSON circuits can manage splitter protection as a single protected circuit. However, for the Y-Cable protection, two OCHCC WSON circuits and two protection groups are required.

Note Cisco EPN Manager can discover the LMP links between a Cisco NCS 2000 series device and a Cisco IOS-XR device.

Optical Channel (OCH) Trail WSON

OCH trail WSON circuits transport the OCHCC WSON circuits. The OCH trail WSON circuit creates an optical connection from the source trunk port to the destination trunk port of the Transponder (TXP), Muxponder (MXP), GE_XP, 10GE_XP, or ITU-T line card. The OCH trail WSON represents the common connection between the two cards, over which all the client OCHCC WSON circuits, SVLAN circuits or STS circuits are carried. Once an OCHCC WSON is created, a corresponding OCH Trail is automatically created. If the OCHCC WSON is created between two TXP, MXP, GE_XP, or 10GE_XP cards, two circuits are created in the CTC. These are:

- One OCHCC WSON (at client port endpoints)
- One OCH trail WSON (at trunk port endpoints)

If the OCHCC WSON is created between two TXPP or two MXPP cards, three circuits are created in the CTC. These are:

- One OCHCC WSON (at client port endpoints)
- Two OCH Trails WSON (at trunk port endpoints). One for the working and other for the protect trunk.

Optical Channel (OCH) Trail Connecting directly IOS-XR Platform Based Devices

Cisco EPN Manager can discover and provision OCH Trail circuits between the trunk ports of IOS-XR platform based devices connected directly.

These circuits have a fixed route and support a limited number of options. For more information, see Create and Provision an OCH Trail Circuit Connecting IOS-XR Platform Based Devices Directly, on page 536.

A managed link must be created between the trunk ports of the devices, to enable circuit provisioning.

An OCH Trail hybrid circuit connects a Cisco IOS-XR device and a Cisco NCS 2000 series device. Cisco EPN Manager can discover such circuits whose trunk ports must be connected via either a manual link or an LMP link to the passive units of Cisco NCS 2000 series devices.

Note Provisioning is not supported for this type of optical circuits.

An OCH Trail hybrid circuit connects a Cisco IOS-XR device to another Cisco IOS-XR device through a Cisco SVO network. Cisco EPN Manager can provision such circuits whose trunk ports must be connected through either a manual link to the passive units of Cisco SVO devices. Discovery of such circuits in EPNM is not supported.

Optical Channel (OCH) Trail Connecting IOS-XR Platform Based Devices through NCS 2000 Devices

Cisco EPN Manager can discover an OCH trail circuit between the trunk ports of IOS-XR platform based devices connected through an NCS 2000 DWDM network.

These OCH trail circuits are read only and are automatically created and removed when the related Media Channel NC circuit is created or removed on the NCS 2000 devices.

This circuits has the following prerequisites:

- An LMP link must be created between the trunk port of each NCS 1004 and the passive port of the NCS 2000. For more information, see Configure GMPLS and WSON Properties, on page 388.

  The LMP termination must be of **NCS 1004 signaling** type.

- The client and trunk ports of the NCS 1004 must be activated. For more information, see Provision Optical Interfaces , on page 360.
- A Media Channel NC must be provisioned via EPNM between the passive ports of the NCS 2000 devices. When provisioning this circuit, the related trunk ports of the NCS 1004 will also be shown. An intermediate NCS 1004 device can be used as a regenerator for this circuit.

If NCS 4000 devices are connected to the client ports of the NCS 1000 with an OTU4 payload, TE links are discovered and they can be used for ODU tunnel circuit routing.

Optical Channel (OCH) Trail Connecting NCS 1002, NCS 55xx, and ASR 9K Devices

Cisco EPN Manager can discover an OCH Trail circuit from the following devices:

- Source trunk port of an NCS 1002 device to the destination trunk port of another NCS 1002 device.
- Source trunk port of an NCS 55xx device (trunk ports on NCS55-6X200-DWDM-S card) to the destination trunk port of another NCS 55xx device.
- Source trunk port of an ASR 9K device (trunk port on ASR9K-400G-DWDM-TR) to the destination trunk port of another ASR 9K device.

The trunk port of each of these devices must be connected via a manual link to the passive units of NCS 2K devices. Where the manual links are terminated, and OCH-NC circuit must be created as a pre-requisite between the ports of the passive units of NCS 2K network.

Note Provisioning is not supported for this type of optical circuits.

Optical Channel (OCH) Trail User-to-Network Interface (UNI)

An OCH trail UNI circuit establishes connectivity between the following devices:

- Cisco NCS 2000 series devices and Cisco NCS 4000 series devices. It provides an end-to-end configuration of DWDM network that consists of Cisco NCS 2000 series devices and terminates on a Cisco NCS 4000 series device. When an OCH trail UNI circuit is created in a Cisco NCS 4016 network element, a corresponding OCHNC circuit is created in the Cisco NCS 2006 network element.

Note You will not be able to modify or delete the OCHNC circuit.

- Cisco NCS 1000 series devices that act as UNI-C and Cisco NCS 2000 series devices that act as UNI-N. The OCH trail UNI circuit originates from an NCS 1002 trunk interface (UNI-C) on the source NCS 1002 node and terminates on the NCS 2000 series interface (UNI-N) on the destination NCS 2000 series node to create an optical connection. The prerequisite for the OCH trail UNI circuit is to create a Link Management Protocol (LMP) link between the optical channel Add/Drop NCS 2000 series interface on the NCS 2000 series node and the NCS 1002 interface on the NCS 1002 node. See Configure GMPLS and WSON Properties, on page 388.

Note Cisco EPN Manager discovers the OCH Trail UNI circuits that originates from NCS 1002 device running on software version 6.3.2.

The LMP link can either be a numbered link or an unnumbered link. An unnumbered link does not have an IP address.

- For unnumbered links, Cisco EPN Manager creates the required explicit path object on the NCS 1000 series device, which is the source device. This device will contain two constraints, one for the source peer NCS 2000 series device and the other for the destination device. You can add more constraints as required.
- For numbered links, a default explicit path object is not required. If you want to add constraints, you must first specify the source NCS 2000 series node in the explicit path even if the node is selected as the source endpoint of the OCH Trail UNI circuit. If you do not add the source NCS 2000 series node as your first constraint, the corresponding OCHNC circuit on the NCS 2000 series node will not be created.

Note You cannot use both numbered and unnumbered links for the same OCH Trail UNI circuit.

Spectrum Switched Optical Network (SSON) Circuits

SSON circuits allow you to provide more than 96 channels in a span. Using the SSON functionality, the circuits are placed closer to each other if they are created within a media channel group. The minimum spacing between circuits is 50 GHz.

SSON circuits can be created only if the source and destination nodes have the SSON package installed.

Note The existing OCHNC, OCHCC, and OCH Trail circuits cannot be upgraded to SSON circuits.

Cisco EPN Manager supports the following SSON circuits:

- Media Channel Circuits—Media channel (MCH) works on any available frequency (flexible frequency) and establishes connection between two optical nodes. A continuous section of the spectrum is allocated between the source and destination nodes. The MCH contains information regarding the allocated optical bandwidth. A media channel can be of three modes:
  - Media Channel Trail—MCH trail SSON circuits transport the MCHCC SSON circuits. These circuits create optical connection between trunk ports of a co-located TXP (based on the carrier trails).
  - Media Channel Network Connection (MCHNC)—MCHNC SSON circuits create optical connection between filter ports (based on the carrier).
  - Media Channel Client Connection (MCHCC)—MCHCC circuits create optical connection between client ports of a co-located TXP.

- Media Channel Group (MCHG)—MCHG is a container that can include one or more media channels. Media channels are grouped together to increase the spectral efficiency. Circuits can be created at closer intervals, when compared to OCH circuits. Maximum number of media channels can be achieved on a single fiber, if the MCHG covers the entire C-band.

Managed Plane Circuits

With SVO devices, Cisco EPNM will support managed plane provisioning. To add SVO devices, see Add SVO Devices, on page 47. We can provision OCH-Trail and OCH-CC on SVO devices. To create and provision OCHCC and OCH-Trail circuits, see Create and Provision an OCH Circuit, on page 529.

Optical Transport Network (OTN) Circuit

OTN specifies a digital wrapper, which is a method of encapsulating an existing frame of data, regardless of the native protocol, to create an optical data unit (ODU), similar to that used in SDH/SONET. OTN provides the network management functionality of SDH/SONET, but on a wavelength basis. A digital wrapper, however, is flexible in terms of frame size and allows multiple existing frames of data to be wrapped together into a single entity that can be more efficiently managed through a lesser amount of overhead in a multi-wavelength system.

The OTN specification includes framing conventions, non-intrusive performance monitoring, error correction (FEC), rate adaption, multiplexing mechanisms, ring protection, and network restoration mechanisms operating on a wavelength basis.

A key element of a digital wrapper is the forward error correction (FEC) mechanism that provides performance gains for improved margins and extended optical reach.

The OTN architecture is compliant to ITU-T G.872. An OTN circuit can be established statically or dynamically between ingress and egress nodes using Resource Reservation Protocol (RSVP) signaling. An OTN circuit is established and maintained as a label switched path (LSP) between the ingress and egress Label Switched Routers (LSRs) switched through transit LSRs. An LSP can be established as a soft permanent connection (SPC) when the request comes from the user interface.

Following are the types of OTN circuits:

- Optical Channel Data Unit User-to-Network Interface (ODU UNI), on page 490
- Optical Channel Data Unit (ODU) Tunnel, on page 491
- Optical Channel Payload Unit (OPU) Over Optical Channel Data Unit (ODU), on page 491
- Optical Channel Data Unit User-to-Network Interface (ODU UNI) Hairpin, on page 492
- Optical Channel Data Unit (ODU), on page 492

Optical Channel Data Unit User-to-Network Interface (ODU UNI)

ODU is the transport container defined to carry client signals from network ingress to egress. The ODU provides a payload area for client data along with performance monitoring and fault management. The payload area of an ODU may contain a single non-OTN signal as a client or may contain multiple lower rate ODUs as clients. An ODU UNI circuit represents the actual end-to-end client service passing through the OTN architecture.

Open Ended ODU UNI

In an open-ended ODU UNI circuit, one or both end points may be connected to ODU subcontrollers, instead of client payload controllers.

Cisco EPN Manager supports three types of open-ended ODU UNIs:

- Only the source interface is an ODU subcontroller
- Only the destination interface is an ODU subcontroller
- Both source and destination interfaces are ODU subcontrollers

To create an open-ended ODU UNI circuit, you must configure ODU subcontrollers on devices before adding the devices to Cisco EPN Manager. Use the **controller oduk** command to configure ODU subcontrollers on devices.

Example: Configure an ODU subcontroller on a Cisco NCS 4000 Device

In this example, two ODU0 subcontrollers are configured to an ODU1 controller.

```
RP/0/RP0:router#conf
RP/0/RP0:router(config)# controller ODU10/1/0/1
RP/0/RP0:router(config-odu1)# tsg 1.25G
RP/0/RP0:router(config-odu1)# ODU0 tpn 1 ts 1
RP/0/RP0:router(config-odu1)#  ODU0 tpn 2 ts 2
RP/0/RP0:router(config-odu1)#commit
```

To verify that the ODU subcontrollers are configured correctly on the device:

```
RP/0/RP0:router#sh controllers ODU0 ?
  0/1/0/0     ODU0 Interface Instance
  0/1/0/1/10  ODU0 Interface Instance
  0/1/0/1/20  ODU0 Interface Instance
  R/S/I/P     Forward interface in Rack/Slot/Instance/Port format
```

After configuring the ODU subcontrollers on the device, you must add the device to Cisco EPN Manager. You can then verify that the ODU0 0/1/0/1/10 and ODU0 0/1/0/1/20 subcontrollers are available in the inventory.

Optical Channel Data Unit (ODU) Tunnel

ODU tunnel circuits transport the ODU UNIs. The ODU tunnel represents the common connection between two Cisco NCS 4000 series devices that are connected with Traffic Engineering (TE) links. Once an ODU UNI circuit is created, a corresponding ODU tunnel is automatically created.

Optical Channel Payload Unit (OPU) Over Optical Channel Data Unit (ODU)

OPU over ODU circuits provide a high-bandwidth point-to-point connection between two customer designated premises. Client signals are mapped over an OTN framing structure with in-band management through GCC0. These circuits uses ODU UNI circuits to carry client signals through the network. You need to perform the following tasks to create and provision an OPU over ODU circuit:

- Using Cisco EPN Manager, create an ODU UNI circuit. For information about how to create ODU UNI circuits, see Create and Provision an OTN Circuit, on page 544.
- Using Cisco Transport Controller (CTC), create LMP links and enable the links on the devices that you want to use in the OPU over ODU circuits. For information about how to create LMP, see the "DLP-K27 Create an LMP Using CTC" section in the OTN and DWDM Configuration Guide for Cisco NCS 4000 Series.

- Using Cisco EPN Manager, create an OPU over ODU circuit with the LMP links enabled devices. For information about how to create OPU over ODU circuits, see Create and Provision an OTN Circuit, on page 544.

Optical Channel Data Unit User-to-Network Interface (ODU UNI) Hairpin

An ODU UNI Hairpin circuit is similar to an ODU UNI circuit, but it is created in the management plane and is an intra node circuit, that is, the source and destination are the same device but with different interfaces. In this type of circuit, the connection is established between two clients or two ODU subcontrollers.

Cisco EPN Manager supports the following types of ODU UNI Hairpin circuits:

- Circuits without open-ended cross-connect—In this type of circuits, the interfaces of source and destination are not OTU interfaces.
- Circuits with open-ended cross-connect on one side—In this type of circuits, the interface of either source or destination is an OTU interface.
- Circuits with open-ended cross-connect on both sides—In this type of circuits, the interface of source or destination are OTU interfaces.

Note Cisco EPN Manager GUI does not support **Edit/Modify** operation on ODU UNI Hairpin service; however, Cisco EPN Manager NBI allows you to perform this operation. **DELETE** and **RECREATE** commands are generated on the device as a part of the Edit/Modify operation through NBI.

Optical Channel Data Unit (ODU)

The Optical Channel Data Unit (ODU) circuit represents the common connection between two Cisco NCS 2000 series devices that are connected with Traffic Engineering (TE) links. The ODU is created as a sub controller of an OTU controller. ODU contains information for the maintenance and operational functions to support optical channels. ODU Over Head (OH) information is added to the ODU payload to create the complete ODUk. The ODUk OH consists of portions dedicated to the end-to-end ODUk path and to six levels of tandem connection monitoring. The ODUk path OH is terminated where the ODUk is assembled and disassembled. The TCM OH is added and terminated at the source and sink to the corresponding tandem connections.

ODU cross connection is an end-to-end channel between two OTN or client ports in the OTN network. Cisco EPN Manager supports ODU cross connections with bidirectional SNC-N protection.

Supported Circuit Emulation Services

Circuit Emulation (CEM) provides a protocol-independent transport over IP networks. It enables proprietary or legacy applications to be carried transparently to the destination, similar to a leased line. In traditional TDM networks, numerous physical circuits are maintained between geographically diverse locations to provide TDM transport. CEM allows TDM endpoints to connect across an IP/MPLS core. In CEM, endpoints are connected to the TDM circuits, but the circuits terminate at each local router that has the IP/MPLS connectivity available. The router then transports those TDM frames across the IP/MPLS core via Circuit Emulation (CEM) pseudowires (PWs) to the remote endpoint that also has the IP/MPLS connectivity available. Thus, the TDM endpoints can communicate as if they were directly connected by physical circuits. Cisco EPN Manager supports the following CEM modes:

- Structure-Agnostic time-division multiplexing (TDM) over Packet (SAToP)—This is the unstructured mode in which the incoming TDM data is considered as an arbitrary bit stream. It disregards any structure that may be imposed on the bit stream. SAToP encapsulates the TDM bit streams as pseudowire (PWs) over PSN.
- Circuit Emulation over Packet (CEP)—This mode is used to emulate Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) circuits and services over MPLS. To transport SONET/SDH circuits through a packet-oriented network, the Synchronous Payload Envelope (SPE) or Virtual Tributary (VT) is broken into fragments. A CEP header and optionally an RTP header are prepended to each fragment.
- Circuit Emulation Service over Packet Switched Network (CESoPSN)—This is the structured mode in which the structured TDM signals are encapsulated as PWs and transmitted over PSN. It selects only valid timeslots and disregards the idle timeslots for transmission. Thus, CESoPSN can save utilized bandwidth.

Cisco EPN Manager supports the following CEM service types depending on the rate at which the circuits can transmit data:

- DS0—A basic digital signal with transmission data rate of up to 64 Kbps.
- T1 and E1—Digital Signal (DS) is known as T-carrier in North America, South Korea, and Japan and as E-carrier in the rest of the world. The T1 circuit has a transmission data rate of up to 1.544 Mbps. The E1 circuit has a transmission data rate of up to 1.984 Mbps in framed mode and 2.048 Mbps in unframed mode.
- T3 and E3—The T3 circuit has a transmission data rate of up to 44.736 Mbps. The E3 circuit has a transmission data rate of up to 34.368 Mbps. The T3 or E3 circuit can transport 672 DS0 level channels and 28 DS1 level channels within its payload.
- VT 1.5—A virtual tributary network line with transmission data rate of up to 1.728 Mbps.
- STS-1—A synchronous transport signal with transmission data rate of up to 51.84 Mbps.
- STS-3c—A synchronous transport signal with transmission data rate of up to 155.52 Mbps.
- STS-12c—A synchronous transport signal with transmission data rate of up to 622.08 Mbps.
- STS-48c—A synchronous transport signal with transmission data rate of up to 2488.32 Mbps.
- VC4—A synchronous Transport Module with transmission data rate of up to 155.52 Mbps.
- VC4-4c—A Synchronous Transport Module with transmission data rate of up to 622.08 Mbps.
- VC4-16c—A Synchronous Transport Module with transmission data rate of up to 2488.32 Mbps.
- VC11—A Virtual Container line with transmission data rate of up to 1.7 Mbps.
- VC12— A Virtual Container line with transmission data rate of up to 2.2 Mbps.

Note On IOS-XE devices, point-to-point services use the **`l2vpn xconnect`** command.

Supported L3VPN Services

An MPLS Layer 3 VPN creates a private IP network. The customer connects to the network via customer edge (CE) routers, which act as IP peers of provider edge (PE) routers.

Virtual Routing and Forwarding (VRFs)

On the PE, Virtual Routing, and Forwarding (VRF) instances act as virtual IP routers dedicated to forwarding traffic for the L3VPN service. The VRFs learn the routes to each other via the Multi-Protocol Border Gateway Protocol (MP-BGP), and then forward traffic using MPLS.

A VPN is composed of at least one but typically several VRFs. Cisco EPN Manager uses the VPN ID to discover which VRFs together form a single VPN. If Cisco EPN Manager discovers an existing network where no VPN ID has been provisioned, it takes all VRFs with the same name and associates them into one VPN. For VPNs created using Cisco EPN Provisioning, which uses a naming convention with version number prefixes and different suffixes, Cisco EPN Manager recognizes the different VRFs as belonging to one VPN.

In general there is a regular expression which can be configured to allow for varying naming convention.

Route Targets (RTs)

The connections between VRFs are defined using Route Targets (RTs) that are imported and exported by the VRFs. Cisco EPN Manager makes it easy to set up a full mesh of connections, and automatically allocates the route target to be used. The route target consists of a prefix which is either an AS number or an IPv4 address, for example, a full mesh prefix, 100 [681682]. The prefix can be selected from the existing BGP autonomous system (AS) numbers in the network, or it can be entered manually. The second number following the prefix is allocated automatically by Cisco EPN Manager.

Alternatively or in addition to the full mesh, it is possible to manually select route targets. During VPN creation, there is an initial screen where you type in the route targets to be used within a VPN, and then for each VRF you can select which route targets you import and export. You also specify for which address family (IPv4 or IPv6) you use the route target. This can be used, for example, to configure extranets, by importing route targets used in other VPNs.

Route Redistribution

The routes that are exchanged between the PE and the CE have to be redistributed into the MP-BGP routing protocol so that remote endpoints can know which prefixes can be reached at each VRF. To control route redistribution, Cisco EPN Manager allows you to define the required protocol (OSPF, Static, Connected, or RIP), the protocol's metric value, and optionally the applicable route policy.

Endpoints

Cisco EPN Manager supports the creation of IP endpoints on Ethernet subinterfaces. It supports selecting untagged encapsulation, or specifying an outer and optionally an inner VLAN, with 802.1q or 802.1ad encapsulation. You can specify both IPv4 and Ipv6 addresses at an endpoint. You can also specify the BGP and OSPF neighbor details to provision BGP and OSPF neighbors between CE and PE.

For information on how to provision L3VPN service using Cisco EPN Manager, see, Provision L3VPN Services, on page 553.

Supported Segment Routing Services

The Cisco EPN Manager supports provisioning of EPL, EVPL, Access EPL, Access EVPL carrier ethernet point-to-point services using Segment Routing traffic engineering(SR-TE) policy. You can modify SR-TE policy during modification of CE services. Related Circuits/VCs tab in Circuit/VCs 360* can be used to view the SR policies associated to this service.

Supported MPLS Traffic Engineering Services

In traditional IP networks, packets are forwarded on a per-hop basis where a route lookup is performed on each router from source to destination. The destination-based forwarding mechanism leads to suboptimal use of available bandwidth between a pair of routers in the network. Mostly, the suboptimal paths are under-utilized in IP networks. To avoid packet drops due to inefficient use of available bandwidth and to provide better performance, traffic engineering (TE) is implemented. TE directs the traffic that is destined to follow the optimal path to a suboptimal path, thus enabling better bandwidth utilization between a pair of routers.

Multiprotocol Label Switching (MPLS) is an integration of Layer 2 and Layer 3 technologies. In an MPLS domain, unique labels are assigned to data packets and the packets are forwarded based on these labels. It avoids the complex lookup in a routing table. MPLS creates a VC switching function to provide similar performance on the IP-based network services as compared to those delivered over traditional networks such as Frame Relay or Asynchronous Transfer Mode (ATM).

By making traditional Layer 2 features available to Layer 3, MPLS enables traffic engineering. MPLS TE enables an MPLS backbone to replicate and expand the TE capabilities of Layer 2 over Layer 3.

MPLS TE uses Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP) across the backbone. The path that an LSP uses is based on the LSP resource requirements and network resources, such as bandwidth and link attributes. Available resources are flooded by means of extensions to a link-state-based Interior Gateway Protocol (IGP). Cisco EPN Manager supports OSPF as the IGP to flood the available bandwidth and link status information across the network. Based on this information, the ingress (headend) router gathers information on all the available resources in the network along with the topology to define tunnels through the network between a set of MPLS-enabled routers. This is called as constraint-based routing. When a shortest path is over-utilized, the IGP automatically routes the traffic to these LSPs. You can also create and provision explicit paths for MPLS TE tunnels.

Cisco EPN Manager provides full path protection mechanism for MPLS TE tunnels against path, link, and node failures. A secondary LSP is established to provide failure protection for the protected LSP that is carrying a tunnel's TE traffic. When there is a failure on the protected LSP, the source router immediately enables the secondary LSP to temporarily carry the tunnel's traffic. If there is a failure on the secondary LSP, the tunnel no longer has path protection until the failure along the secondary path is cleared.

Cisco EPN Manager supports the following MPLS TE service types:

- Unidirectional TE Tunnel, on page 496
- Bidirectional TE Tunnel, on page 496
- MPLS TE 3 Link, on page 496

Unidirectional TE Tunnel

MPLS TE tunnels are unidirectional tunnels that connect a pair of LSRs. Once the unidirectional tunnel is created, a label is assigned for the tunnel that corresponds to a specific path in a MPLS network. The traffic is routed through the tunnel. You must create another unidirectional tunnel between the same routers to route the return traffic. For example, router A is the head end and router B is the tail end of tunnel 1, which is a unidirectional tunnel. You must create another unidirectional tunnel, say tunnel 2 with router B as the head end and router A as the tail end.

Bidirectional TE Tunnel

Two unidirectional TE tunnels established between a pair of LSRs that are connected to each other, can be bound together to form a bidirectional co-routed TE tunnel. The binding of unidirectional tunnels is based on the source and destination addresses, global ID, association ID, and association address of the tunnels. For example, router A and router B that are connected by two unidirectional tunnels, tunnel C and tunnel D, can be bound together to form a bidirectional TE tunnel only if the following conditions are met:

- The source address of tunnel C is the destination address of tunnel D and vice versa.
- The global ID, association ID, and association address of tunnel C and D are the same. The association ID and association address for the tunnels are system-defined and you need to assign a global ID for the tunnels.

Bidirectional TE tunnels inherit the security features of RSVP-TE.

MPLS TE 3 Link

To enable traffic engineering links between two devices, you need to configure the following on both ends of the devices:

- Loopback interface
- Ethernet interface
- BDI Interface
- OSPF, RSVP, and MPLS
- IS-IS and BGP

You can perform these configurations using the MPLS TE 3 link provisioning feature in Cisco EPN Manager.

Supported Serial Services

In a serial communication, the serial port sends and receives bytes of information one bit at a time. The serial communication can be used over longer distances. The cabling between devices can extend up to 1200 meters. Serial communication is used to transmit ASCII data. Communication is completed using three transmission lines—ground, transmit, and receive. Since serial is asynchronous, the port is able to transmit data on one line while receiving data on another. Other lines are available for handshaking, but are not required.

Cisco EPN Manager supports the following serial service types:

- RS232—is a standard communication protocol that links devices in a network to allow serial data exchange. It defines the voltage for the path used for data exchange between the devices. It specifies common voltage, signal level, common pin wire configuration, and minimum amount of control signals. The RS232 interface is suitable for short-distance and low-speed requirements. RS232-RS422 point to point services can be configured by selecting corresponding media-types during configuration of RS232 and RS422 Services.
- RS485—is an EIA/TIA standard that defines a communication bus that is used to form simple networks of multiple devices. The RS485 interface can be used in simplex or half-duplex modes with a single-pair cable. Full-duplex or simultaneous transmit and receive operations can be implemented with a two-pair cable. This interface is used for high speed over long distances.
- RS422—is an EIA/TIA standard that was designed for greater distances and higher baud rates than RS232. To enable high-speed data to be transmitted over serial data lines, RS422 accommodates data rates of up to 100kbps and distances up to 4000 ft. RS422 uses differential transmitters and receivers to balance the transmission techniques. To enable the usage of differential driver, RS422 uses a four conductor cable. Additionally up to ten receivers can be placed on a single cable, providing a multi-point network or bus.
- Raw Socket—is a method for transporting serial data through an IP network. Raw Socket transports Supervisory Control and Data Acquisition (SCADA) data from Remote Terminal Units (RTUs). Raw Socket supports point-to-point and point-to-multipoint connections. Raw Socket supports point-to-multipoint connection over an asynchronous serial line and has a built-in auto TCP connection retry mechanism. You can choose Synch RS232, RS422 P2MP options while configuring Raw Socket by selecting Synch and media-type options.

Circuit/VC Discovery Overview

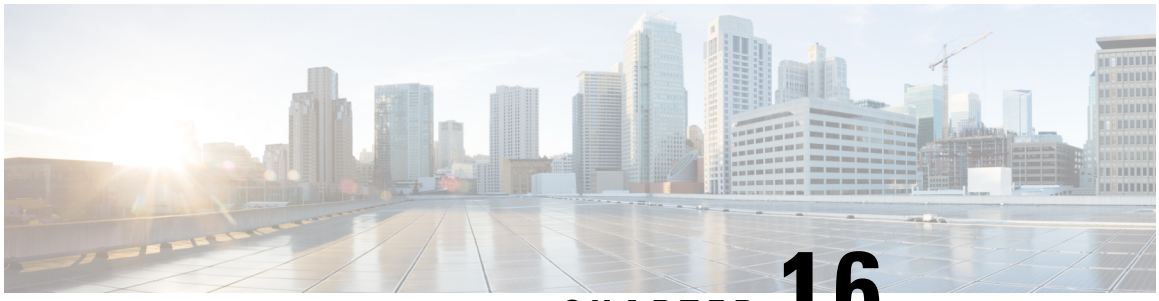
Cisco EPN Manager uses the Service Discovery feature to automatically discover circuits/VCs existing in the network. Ensure that the Service Discovery feature is enabled under **Administration** > **Settings** > **System Settings**. See Enable and Disable Service Discovery, on page 619.

Circuit/VC discovery depends on device-level inventory discovery, and consists of two parts:

- Resource facing service (RFS) discovery—The RFS represents the relations between resources on different devices. During RFS discovery, the system creates device-level objects and network-level objects. Device-level RFS objects represent the circuit/VC configuration parts of the device-level configuration. Network-level RFS objects aggregate device or other network-level objects to represent network-level entities.
- Customer facing service (CFS) matching—The CFS represents the customer facing data for a circuit/VC. The CFS is derived from discovered RFS and represents the endpoints of the circuit/VC in the network. During CFS discovery, the system creates CFS objects for the discovered RFS objects.

Discovery is an ongoing process in Cisco EPN Manager. When you first start using Cisco EPN Manager, the circuits/VCs that exist in the network are discovered. Later, when you start provisioning circuits/VCs using the Provisioning Wizard, Cisco EPN Manager will discover the provisioned circuits/VCs and will search for a match between the resources used in the circuit/VC and the resources discovered from the network. When a match is found between a discovered circuit/VC and a provisioned circuit/VC, information from the provisioned CFS is copied into the discovered CFS.

Cisco EPN Manager allows you to compare between the provisioned and discovered versions to identify changes that might have been made in the device configurations and you can do a reconciliation, if necessary. See Compare and Reconcile Provisioned and Discovered Versions of a Circuit/VC, on page 647



CHAPTER 16

Provision Circuits/VCs

Provision Circuits/VCs in Cisco EPN Manager

The process of creating and provisioning a circuit/VC is similar for all the supported technologies and involves:

- Specifying the endpoints of the circuit/VC.
- Defining the configuration parameters of the circuit/VC.

To create and provision a new circuit/VC:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click on the **Device Groups** button, select the required device group(s) and click **Load**.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click the **Circuits/VCs** tab.

Step 5 Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Note You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**

Step 6 From the **Technology** drop-down list, choose the required technology. For example, if you are creating a circuit for Optical/DWDM network, choose **Optical**.

Step 7 In the **Service Type** area, choose the type of circuit/VC you want to create. For example, if you are creating a circuit/VC for Optical/DWDM network, the various circuit types include OCHNC WSON, OCHCC WSON, OCH-Trail WSON, OCH-Trail UNI, ODU UNI, ODU Tunnel, and OPU over ODU.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the Customer Service Details page.

Step 10 (Optional) Select the customer for whom the circuit/VC is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then go to the Provisioning Wizard to start provisioning the circuit/VC.

Step 11 Enter the service name and its description.

Step 12 From the **Deployment Action** drop-down list, choose the action that you want to perform after defining the attributes for the circuit/VC. The options are:

- **Preview**—Displays the generated CLIs for each device. You can review the CLIs and decide if you want to edit any attributes or go ahead with the deployment.
- **Deploy**—Deploys the configuration to the relevant devices immediately after you click **Submit** in the last page of the Provisioning Wizard.

  Click one of the following deployment options:

  - **Deploy Now**—Directly deploys the provisioning order
  - **Deploy Later**—Saves the created provisioning order.You can deploy the same order at later point of time.To redeploy the provisioning order click the circuit/VCs link at the bottom of the left pane.
  - **Schedule Deployment**—Saves the order for future deployment at the designated time provided by you. Schedules the provisioning order and creates the Job order to be deployed at the scheduled time. If required, you can specify the date and time to provision the order in the Job Scheduler.dialog box.

    If you click this **Schedule Deployment** radio button, specify the following:

    - **Deploy Schedule Time**—Specify a schedule time for deployment of provision order.
    - **Server Time**—Displays the current server time.

To know more about how to schedule and save a provisioning order, see Save and Schedule a Provisioning Order, on page 579

Step 13 Click **Next** to choose the endpoints and define the attributes based on the technology you have selected.

Step 14 Click **Submit**. Depending on the deployment action you have chosen, the relevant action will be performed. That is, if you have chosen to preview the configuration, the preview page will be displayed where you can view the configurations, and then click **Deploy**. If you have chosen to deploy, the configurations will be directly deployed to the relevant devices.

Step 15 (Optional) Click the **Leave this View** button to continue using Cisco EPN Manager and to enable the service deployment to continue in the background.

Note If the device is busy, the request from Cisco EPN Manager to deploy the service will wait up to a pre-configured period of time before the request times out. To change this setting, see Set the Service Deployment Timeout Value, on page 501.

The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the i icon next to the circuit/VC name to see the Circuit/VC 360 view.

For information about how to create and provision circuit/VCs for various technologies, see:

- Provision EVCs in a Carrier Ethernet Network, on page 507
- Provision Circuits in an Optical/DWDM Network, on page 526
- Provision L3VPN Services, on page 553
- Provision Circuit Emulation Services, on page 573
- Provision MPLS Traffic Engineering Services, on page 582

You can view the saved provisioning order in the Planned Circuits/VCs tab from **Administration** > **Dashboards** > **Job Dashboard** > **Provisioning**.

Click the (I) icon at the **Last run stat** field and view the configuration and Device details.

Set the Service Deployment Timeout Value

When you deploy a service to devices, if the devices are pre-occupied or busy, the service request created waits for a pre-configured period of time to acquire a ‘device lock’ for deploying the service. By default, the timeout value is set to 60 minutes.

To change the default timeout value:

Step 1 From the left sidebar, choose **Administration > Settings > System Settings**.

Step 2 Expand the **Circuits/VCs** section and click **Deployment Settings**.

Step 3 Set the required timeout value in minutes.

Cisco EPN Manager will now wait up to the specified time period to acquire the device lock for deploying the service. If the lock is not acquired within this time, the service deploy operation will fail.

Set the Circuit Activation Wait Timeout Value

You can configure the maximum time interval for which the provisioning system waits until circuit activation wait timeout.

Step 1 From the left sidebar, choose **Administration > Settings > System Settings**.

Step 2 Expand the **Circuits/VCs** section and click **Deployment Settings**.

Step 3 Set the required timeout value in minutes in the **Circuit Activation Wait Timeout** field.

By default, the timeout is 5 minutes.

Configure to Auto Delete WSON/SSON Circuits

You can enable the option to auto delete the NCS2K TL1 based WSON/SSON circuits that EPNM manages. If the circuits are deleted from other devices or CTC, it is also deleted from EPNM. To configure auto delete WSON/SSON circuits:

Step 1 From the left sidebar, choose **Administration > Settings > System Settings**.

Step 2 Expand the **Circuits/VCs** section and click **Deployment Settings**.

Step 3 Check the **Auto delete WSON/SSON circuits** check box.

What Happens When a Deployment Fails

When you deploy a circuit/VC, Cisco EPN Manager performs configuration changes in the participating devices based on the type of circuit/VC. Only when the configuration changes are successfully deployed to the devices, the circuit/VC will be considered as successfully provisioned. If the deployment of configuration changes fails in any one of the participating device, Cisco EPN Manager rolls back the configuration changes made so far in all the devices.

If the deployment of configuration changes fails in any one of the participating device, you can click **Redeploy** on the provisioning wizard. The redeploy action reattempts the deployment with the same configuration.

Note Redeploy button is supported for OCHNC WSON, OCHCC WSON, OCHCC, OCH-Trail WSON, OCH-Trail, Media Channel NC SSON, Media Channel Trail SSON, Media Channel CC SSON optical circuits.

Deployment action can result in any one of the following scenarios:

- Deployment succeeds in all the participating devices; roll back is not initiated—In this scenario, all devices are successfully configured and the circuit provisioning is successful.
- Deployment fails; roll back is initiated and succeeds—In this scenario, when configuring multiple devices, the configuration fails in one of the device. The failure could be due to various reasons, for example, the device has declined the configuration. Cisco EPN Manager identifies the failure and successfully rolls back all the configuration changes that were made on all the devices. In this scenario, all device configurations are restored to the states, which were there before the deployment was attempted.

  Here is an example with three devices, A, B, and C, which are configured in a sequential order to provision a circuit. The configuration changes are deployed successfully in device A, but the deployment fails in device B. Cisco EPN Manager detects the failure and stops further configuration in devices B and C. It rolls back the configuration in the reverse order of provisioning, that is, it first rolls back the device B, followed by device A. Following are the actions that are performed sequentially in the three devices:

  - Device C—Rollback is not required for device C because there were no changes deployed to the device. This is because the configuration failure was detected in device B before configurations changes were sent to device C.

- Device B—Cisco EPN Manager checks if there are any configuration changes made on this device before the deployment failed. If there are any changes, the partial configuration on this device is removed and the device is rolled back to the previous configuration.
- Device A—Cisco EPN Manager performs a complete roll back in device A, where all the configuration changes that were successfully deployed earlier are removed and the device is rolled back to the previous configuration.

- Deployment fails; roll back is initiated but fails— In this scenario, when the configuration deployment fails on any of the participating device(s), Cisco EPN Manager performs a rollback, but the rollback on one or more devices fail. Now, the device(s) on which the roll back had failed, has the partial configuration.

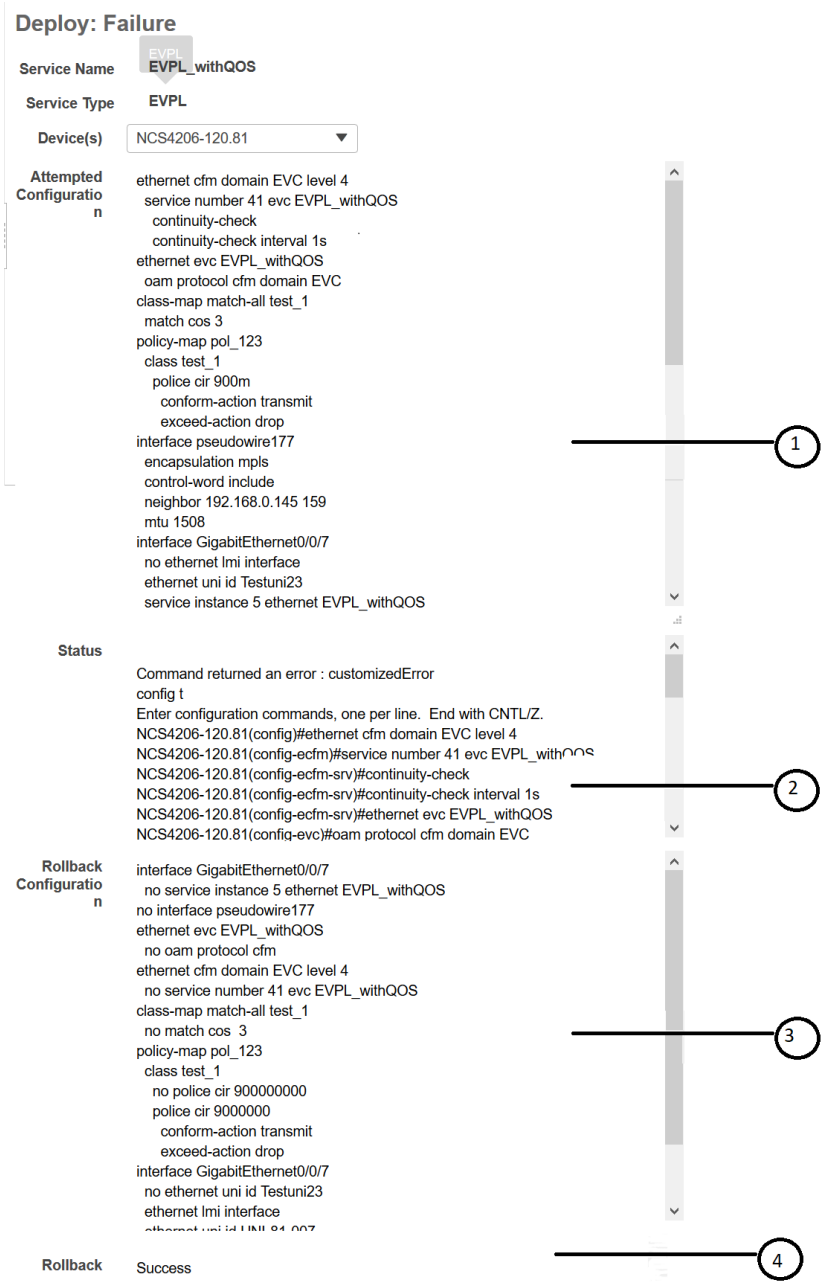
  For example, the configuration changes are successfully deployed in devices A and B, the deployment fails in device C. Cisco EPN Manager identifies the failure and initiates the rollback in the reverse order of provisioning, that is, it first rolls back the device C, device B, and then device A. Following are the actions that are performed sequentially in the three devices:

  - Device C—Cisco EPN Manager performs a successful rollback in device C.
  - Device B—When attempting a rollback on device B, device connectivity is lost and there could be partial configurations left on the device.
  - Device A—Cisco EPN Manager performs a rollback of Device A, even if the roll back fails in device B.

Note The rollback may fail due to various other reasons.

In the Provisioning Wizard, after previewing the configurations, click **Deploy**. When the deployment fails, the rollback configuration and the status for each participating device is displayed. From the **Device(s)** drop-down list, choose the device for which you want to view the rollback configuration and the status.

The following figure illustrates the rollback configuration and the rollback status for each device.



1	Attempted Configuration— Shows the configurations that were deployed to the device selected in the **Device(s)** drop-down list.
2	Deployment Status— Shows the deployment status of the selected device. If the deployment succeeds, it shows the status as "Success". If the deployment fails, it provides information about the failure.
3	Roll back Configuration— Shows the configurations for which rollback is automatically attempted.

4	Roll back Status— Shows the rollback status of the selected device. If the rollback succeeds, it shows the status as "Success". If the rollback fails, it provides information about the failure. You can use this information to manually clean up the partial configurations on the device.

You can also delete the failed deployments from this window by clicking **Delete**.

You can also click the *i* icon next to the **Provisioning** column in the Circuits/VCs and Deleted Circuits/VCs tabs in the extended tables to view the details of configuration, configuration errors, rollback configuration, and rollback configuration errors for each device participating in the circuit/VC. The *i* icon is available for all provisioning states, except None. For information about how to access the extended tables, see View Detailed Tables of Alarms, Network Interfaces, Circuits/VCs, and Links from a Network Topology Map, on page 175.

For information about how to troubleshoot deployment and rollback failures, see Troubleshoot Configuration Deployment Failures and Roll Back Failures, on page 505.

Troubleshoot Configuration Deployment Failures and Roll Back Failures

Following are the tips to troubleshoot the deployment or roll back failures:

- Deployment fails, but roll back succeeds— If the configuration deployment fails, roll back is automatically initiated and the results are displayed in the results page. Analyze the attempted configuration and error message shown in the results page for each device and identify the root cause of the deployment failure.

  The deployment failure could be due to, but not limited to the following issues:

  - Invalid values entered for the service parameters in the Provisioning Wizard. For example, the Service ID may already exists or there could be semantic errors in the CLI that is generated, and so on.
  - Device issues such as, device is not reachable, device password has changed, and so on.

  In this case, you must locate the circuit (by the name that you had given when creating it) for which deployment has failed, edit the circuit, and re-attempt the provisioning. If the service parameter for which the value to be changed is not editable, delete the circuit and create a new circuit.

Note Before deleting the circuit, ensure that it is not in use.

- Both, deployment and roll back fails— In this case, do the following:
  1. Ensure that the device is reachable and perform a device re-synch.
  2. If there were any device issues that were reported in the previous deployment, try to fix the issues.
  3. Edit the circuit and update the attributes, if required, and then re-attempt the circuit deployment.
  4. If the deployment fails, Cisco EPN Manager will initiate the roll back.
  5. If the roll back fails again, identify the cause of the roll back failure.
  6. To identify the cause of the failure, you can use the configuration and roll back transaction details, history of the service deployment attempts, and the roll back attempts that are displayed in the Circuit/VC 360 view. See Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 629.

7. Manually remove the partial configurations that are stored on the device.

You can also contact the Cisco representative to analyze and identify the root cause of configuration deployment failure and roll back failure.

WAN Automation Engine Integration

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 7.1.1 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, on page 589.

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, on page 597 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.

Provision EVCs in a Carrier Ethernet Network

Summary of Cisco EPN Manager Carrier Ethernet Provisioning Support

This topic provides a summary of the Carrier Ethernet service provisioning support in Cisco EPN Manager. For a more detailed overview of the different types of EVCs and the supported underlying networks, see Overview of Circuit/VC Discovery and Provisioning, on page 479.

Cisco EPN Manager supports provisioning of port-based and VLAN-based VCs of the following types:

- E-line—Ethernet Private Line (EPL) and Ethernet Virtual Private Line (EVPL). See E-Line, on page 481.
- E-LAN—EP-LAN and EVP-LAN. See E-LAN, on page 482.
- E-Access—Access EPL and Access EVPL. See E-Access, on page 483.
- E-TREE—EP-TREE and EVP-TREE. See E-Tree, on page 483.
- EVPN Virtual Private Wire Service (VPWS). See EVPN Virtual Private Wire Service (VPWS), on page 484.

Cisco EPN Manager supports the following supplementary provisioning functions that can be used during EVC creation:

- Provision UNIs—For each EVC, you must define the attributes of the participating UNIs. You can either do this during the EVC creation or you can provision a UNI independently of the EVC creation process. See Configure a Device and Interface To Be a UNI, on page 520.
- Provision ENNI—For E-Access circuits, you must define the attributes of the ENNI. You can either do this during the EVC creation or you can provision an ENNI independently of the EVC creation process. See Configure a Device and Interface To Be an ENNI, on page 521.

- EVC Attribute Profiles—You can create profiles containing all the required attributes for an EVC. These profiles can be selected during EVC creation to define the attributes of the EVC, instead of having to define the attributes individually for each EVC. See Create Circuit/VC Profiles , on page 607.

Prerequisites for EVC Provisioning

The following prerequisites must be met before you can provision EVCs:

1. Communication between devices must be set up before you can provision EVCs:
   - In an MPLS end-to-end network, Label Distribution Protocol (LDP) must be set up across the network and each device must be provided with an LDP ID. This enables peer label switch routers (LSRs) in an MPLS network to exchange label binding information for supporting hop-by-hop forwarding. Alternatively MPLS end-to-end connectivity can be achieved using MPLS Traffic Engineering or segment routing, and specifically, EVC (only P2P type) provisioning over unidirectional or bidirectional TE tunnels is supported. CEm provisioning over TE tunnels and provisioning over SR policies is also supported.
   - If there is Ethernet access, that is, not all devices are MPLS-enabled, G.8032 rings or ICCP-SM must be configured to connect the Ethernet access switch to the MPLS switch.
   - CDP or LLDP must be configured on the links within the G.8032 ring to enable Ethernet link discovery.
2. To provision EVCs over ICCP-SM and G.8032 networks, all VLANs (1–4095) should be configured either as primary or as secondary VLANs.
3. Inventory collection status for the devices on which the EVCs will be provisioned must be *Completed.* To check this, go to **Inventory > Device Management> Network Devices**, and look at the status in the Last Inventory Collection Status column.
4. Customers can be created in the system so that you can associate a circuit/VC to a customer during the circuit/VC creation and provisioning process. Choose **Inventory > Other > Customers** in the left sidebar to create and manage customers.
5. For interfaces to be used in EVCs, it is recommended to reset the default configuration on the interfaces. In global configuration mode, configure the following command on each interface:

   ```
   default interface 'interface-name'
   ```
6. To provision EPL and EVPN services when using EVPN, define the following command under BGP section in device configuration. If you do not configure this command, the device will not be displayed when you provision an EVPN service.

   ```
   address-family l2vpn evpn
   ```

Create and Provision a New Carrier Ethernet EVC

EVCs are created in the context of the topology map. You can access the topology map and the Provisioning Wizard by choosing **Configuration** > **Network** > **Service Provisioning** in the left sidebar or you can open the Provisioning Wizard from the topology map, as described in the procedure below.

The process of creating and provisioning an EVC is similar for all supported EVC types and involves:

- Specifying the endpoints (UNIs and ENNIs) of the EVC.
- Defining the configuration parameters of the circuit/VC.

After a service is provisioned, you can edit the service and update or change the A-end or Z-end points.

Endpoint modification is supported with E-line services such as EPL and EVPL. you can modify only managed endpoints and full and partial services.

During modification of service, if existing UNI has different device or same device with different port, you can change to other existing UNI.

Some limitations are:

- You cannot modify the endpoints on both end in a single modification of services.
- Create an UNI using the standalone UNI wizard and use it in modification of EPL or EVPL services.
- During modification of service you cannot create a new UNI.

Before you begin

For information about the prerequisites that must be met before you can provision EVCs, see Prerequisites for EVC Provisioning, on page 508.

To create a new EVC:

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the Device Groups button in the toolbar and select the group of devices you want to show on the map.

Step 3 In the Circuits/VCs tab, click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Step 4 Select **Carrier Ethernet** in the Technology drop-down list. Cisco EPN Manager displays a list of relevant circuit/VC types in the Service Type area. For example, Carrier Ethernet service types include EPL, EVPL, EP-LAN, and so on.

Step 5 In the Service Type list, select the type of circuit/VC you want to create.

Step 6 If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 7 Click **Next** to go to the Service Details page.

Step 8 (Optional) Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 9 Enter the Service Details. See Service Details Reference, on page 515 for descriptions of the fields and attributes.

Step 10 For E-Line, E-Tree, and E-LAN EVCs: If required, configure the service OAM which enables fault and performance monitoring across the EVC. For E-Line EVCs, select the Enable CFM check box to enable the Service OAM options. You can then choose to either create a new CFM domain or select an existing domain for the E-Line EVC. See Service OAM, on page 519. Click the Plus icon to add a row to the Service OAM table and provide values in the relevant columns. For E-Tree EVCs, you must specify the direction, i.e., Leaf-to-Root, Root-to-Leaf, or Root-to-Root.

If you want to promote and reconcile point-to-point services or multipoint services, for example EVPL/EPL services, enable the CFM parameters such as CFM Domain name, CFM Domain level, Maint. Assoc. Name Type, ITU Carrier Code, ITU MEG ID Code and Continuity check interval fields. CFM parameters will be read from the discovered version during service promotion. You can perform reconciliation with discovered or provisioned version.

Note By default IEEE is selected as the Maint Assoc Name. If ITU is selected in the Maint. Assoc. Name Type drop down list, ITU Carrier Code and ITU MEG ID code appears.

Step 11 In the Deployment Action field, specify what you want to do when the EVC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

Step 12 Click **Next** to go to the page(s) in which you define the UNI(s). In the case of E-Access, there is an additional page for defining the ENNI.

Step 13 Identify the device and interface that will serve as the UNI:

Note If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, select the Unmanaged check box and provide information for the unmanaged device. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 609.

- If you have already configured the required interface on the device as a UNI, uncheck the **Create New UNI** check box and select the relevant UNI Name from the list.

  Note The UNI names in the list vary according to the services and the options selected at the time of creating the UNI.

  - For EPL, Access EPL, EP LAN, and EP Tree services, only those UNIs for which the **All To One Bundling** option was selected at the time of creation will be listed.
  - For EVPL, Access EVPL, and EVP Tree services, only those UNIs for which the **Multiplexing** or **Bundling** options or both are selected at the time of creation will be listed.

- To create a new UNI:
  - Make sure that the **Create New UNI** check box is checked.
  - In the UNI Name field, enter a name for the UNI that will enable easy identification of the UNI.
  - Select a device from the list in the Device field or click on a device in the map to select it and populate the Device field. A list of the selected device's ports is displayed.
  - Select the required port from the Port table. If the port cannot be used for the UNI, there is an alert icon next to the UNI name in the Port table that displays the reason why the port cannot be selected.

  Note The device you select during UNI creation is circled in orange in the map. The UNI name is displayed above the orange circle. If it is a point-to-point EVC, the orange circle is labeled to indicate whether it is an A-side or Z-side endpoint.

Step 14 If you are creating a new UNI, enter the New UNI Details. See New UNI Details Reference, on page 516 for descriptions of the fields and attributes.

Step 15 Enter the UNI Service Details. See UNI Service Details Reference, on page 517 for descriptions of the fields and attributes.

Step 16 For E-LAN and E-TREE EVCs with H-VPLS as the core technology, select the devices that will serve as the primary and secondary hubs.

Step 17 For E-Line EVCs: In the Pseudowire Settings page, you can select a TE tunnel over which the EVC will traverse, as follows:

a. Check the **Static Preferred Path** check box to assign a static route for the service.

b. Choose the Preferred Path Type as Bidirectional or Unidirectional or SR Policy.

c. Select the required bidirectional TE tunnel from the Preferred Path drop-down list. This list contains all existing bidirectional TE tunnels between the endpoints of the EVC.

Note This field is available only if you selected **Bidirectional** as the Preferred Path Type.

d. Select the required unidirectional TE tunnels from the Preferred Path (A-Z) and Preferred Path (Z-A) drop-down lists.

Note These fields are available only if you selected **Unidirectional** as the Preferred Path Type.

e. Select the **Allow Fallback to LDP** check box if you want the default path to be used if the preferred path is unavailable.

Note If no tunnel exists between the endpoints, the Preferred Path and the Fallback to LDP options will be disabled.

f. Select the **Send Control Word** check box if you want a control word to be used to identify the pseudowire payload on both sides of the connection.

g. Select the **Interworking Option** if you need to interconnect sites using either Ethernet, VLAN, or IP. This option must be enabled if one of the endpoints in the EVC is an unmanaged device.

h. Enter the required bandwidth for the pseudowire.

i. In the **PW ID** field, enter an identifier that is displayed in the Pseudowire settings for point-to- point services.

Note Pesudowire (PW) ID is automatically allocated from the resource pool of PW ID. You can modify the PW ID value only when you create a service. You cannot edit this value during modification of an EVC service. If the entered PW ID is already allocated to the service then an error message is displayed.

Step 18 (Optional) If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the Service Template page. See Extend a Circuit/VC Using Templates, on page 609 for more information.

Step 19 When you have provided all the required information for the circuit/VC, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

Step 20 The circuit/VC should be added to the list in the Circuits/VCs tab in the Network Topology window.

If the configuration deployment fails, see the What Happens When a Deployment Fails, on page 502 section.

Create and Provision a New Carrier Ethernet EVC using EVPN VPWS Technology

To create and provision a carrier ethernet EVC with EVPN:

Before you begin

For information about the prerequisites that must be met before you can provision EVCs, see Prerequisites for EVC Provisioning, on page 508.

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the Device Groups button in the toolbar and select the group of devices you want to show on the map.

Step 3 In the Circuits/VCs tab, click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Step 4 Select **Carrier Ethernet** in the Technology drop-down list. Cisco EPN Manager displays a list of relevant circuit/VC types in the Service Type area. EVPN is supported by Carrier Ethernet service types EPL and EVPL.

Step 5 In the Service Type list, select the type of circuit/VC you want to create.

Step 6 If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 7 Click **Next** to go to the Service Details page.

Step 8 (Optional) Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory > Other > Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 9 Enter the Service Details. See Service Details Reference, on page 515 for descriptions of the fields and attributes.

Step 10 Select the **Use EVPN** checkbox.

Step 11 For E-Line EVCs: If required, configure the service OAM which enables fault and performance monitoring across the EVC. Select the Enable CFM check box to enable the Service OAM options. You can then choose to either create a new CFM domain or select an existing domain for the E-Line EVC. See Service OAM, on page 519. Click the Plus icon to add a row to the Service OAM table and provide values in the relevant columns.

Note ICC based CFM is not supported for EVPN.

Step 12 In the Deployment Action field, specify what you want to do when the EVC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

Step 13 Identify the device and interface that will serve as the UNI:

Note EVPN does not support unmanaged devices.

If you select the **Use EVPN** check-box on the Service Detail page, only the devices supporting EVPN is displayed on the UNI A and Z pages.

- If you have already configured the required interface on the device as a UNI, uncheck the **Create New UNI** check box and select the relevant UNI Name from the list.

  Note The UNI names in the list vary according to the services and the options selected at the time of creating the UNI.

  - For EPL, Access EPL, EPE LAN, and EP Tree services, only those UNIs for which the **All To One Bundling** option was selected at the time of creation will be listed.
  - For EVPL, Access EVPL, and EVP Tree services, only those UNIs for which the **Multiplexing** or **Bundling** options or both are selected at the time of creation will be listed.

- To create a new UNI:
  - Make sure that the **Create New UNI** check box is checked.
  - In the UNI Name field, enter a name for the UNI that will enable easy identification of the UNI.
  - Select a device from the list in the Device field or click on a device in the map to select it and populate the Device field. A list of the selected device's ports is displayed.
  - Select the required port from the Port table. If the port cannot be used for the UNI, there is an alert icon next to the UNI name in the Port table that displays the reason why the port cannot be selected.

Note The device you select during UNI creation is circled in orange in the map. The UNI name is displayed above the orange circle. If it is a point-to-point EVC, the orange circle is labeled to indicate whether it is an A-side or Z-side endpoint.

Step 14 If you are creating a new UNI, enter the New UNI Details. See New UNI Details Reference, on page 516 for descriptions of the fields and attributes.

Step 15 Enter the UNI Service Details. See UNI Service Details Reference, on page 517 for descriptions of the fields and attributes.

Step 16 For E-Line EVCs: On the EVPN Settings page:

a. The **EVPN Instance (EVI) ID** is pre populated. If required, you can modify this value.

b. You can specify the RD Value by deselecting the Auto RD check-box.

c. You can specify the Import RT and Export RT value by deselecting the Auto RT check-box.

Note The Import RT, Export RT, RD and Control Word are editable when the used EVI ID is not associated to any other service.

d. Select the **Control Word** check-box if you want a control word to be used to identify the payload on both sides of the connection.

e. The Z-End AC Identifier and A-End AC Identifier are pre populated. If required, you can modify these values.

f. You can select the **Static Preferred Path** check-box to specify the A to Z or Z to A Preferred Path and specify the SR Policy.

g. Select the Allow Fallback to LDP check box if you want the default path to be used if the preferred path is unavailable.

Note If no tunnel exists between the endpoints, the Preferred Path and the Fallback to LDP options will be disabled.

Step 17 (Optional) If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the Service Template page. See Extend a Circuit/VC Using Templates, on page 609 for more information.

Step 18 When you have provided all the required information for the circuit/VC, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

Step 19 The circuit/VC should be added to the list in the Circuits/VCs tab in the Network Topology window.

Create and Provision an EVC with Multiple UNIs

Cisco EPN Manager supports creating/selecting multiple UNIs during the creation and provisioning of multipoint EVCs (E-LAN and E-Tree).

Note You can have multiple UNIs on the same device for EVCs using VPLS as the core technology, but not for H-VPLS-based EVCs.

Before you begin

For information about the prerequisites that must be met before you can provision EVCs, see Prerequisites for EVC Provisioning, on page 508.

To create a new EVC:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2 From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.

Step 3 Click the **Circuits/VCs** tab.

Step 4 From the **Circuits/VCs** pane toolbar, click the **+** (**Create**) icon.

The Provisioning Wizard opens in a new pane to the right of the map.

Step 5 Select **Carrier Ethernet** in the Technology drop-down list

Step 6 In the Service Type list, select a multipoint EVC type.

Step 7 If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 8 Click **Next** to go to the Service Details page.

Step 9 Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 10 Enter the Service Details. See Service Details Reference, on page 515 for descriptions of the fields and attributes.

Step 11 In the Deployment Action field, specify what you want to do when the EVC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

Step 12 Click Next to go to the page(s) in which you define the UNI(s).

Step 13 In the Multi UNI area, click the Plus icon to add the first UNI to the table. The UNI is given a default name and is automatically selected in the table. Each time you click the Plus icon, a new UNI is added to the table.

Alternatively, you can click on devices in the map to add new UNIs to the table. In this case, the device name will be populated in the Device field under New UNI details.

Step 14 Select a UNI in the table to define or edit its attributes.

Step 15 Identify the device and interface that will serve as the UNI:

- To use an existing UNI, uncheck the Create New UNI check box and select the relevant UNI Name from the list.

  Note The UNI names in the list vary according to the services and the options selected at the time of creating the UNI.

  - For EPL, Access EPL, EP LAN, and EP Tree services, only those UNIs for which the **All To One Bundling** option was selected at the time of creation will be listed.
  - For EVPL, Access EVPL, and EVP Tree services, only those UNIs for which the **Multiplexing** or **Bundling** options or both are selected at the time of creation will be listed.

- To define a new UNI:
  - Make sure that the Create New UNI check box is checked.

- In the UNI Name field, enter a name for the UNI that will enable easy identification of the UNI.
- Select a device from the list in the Device field. A list of the selected device's ports is displayed.
- Select the required port from the Port table. If the port cannot be used for the UNI, there is an alert icon next to the UNI name in the Port table that displays the reason why the port cannot be selected.

Step 16 If you are creating a new UNI, enter the New UNI Details. The New UNI details are relevant for the UNI that is currently selected in the Multi UNI table. See New UNI Details Reference, on page 516 for descriptions of the fields and attributes.

Step 17 Enter the UNI Service Details. See UNI Service Details Reference, on page 517 for descriptions of the fields and attributes. Click Next.

Step 18 If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, provide information for the unmanaged device in the Unmanaged page. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 609

Step 19 Optional. If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the Service Template page. See Extend a Circuit/VC Using Templates, on page 609 for more information.

Step 20 When you have provided all the required information for the circuit/VC, click Submit. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

Step 21 The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window.

Service Details Reference

The following table lists and describes the attributes that define the EVC on the service level. Note that not all attributes are relevant for all the EVC types.

Table 32: Service Details

Attribute	Description
Service Name	Unique name to identify the circuit/VC.
Service Description	Description of the VC that will help to identify the VC.
Service Type	Prepopulated based on the type of service you are creating—EPL, EVPL, EP-LAN, and so on.
Use EVPN	Enables you to create EVPN based connections.
Service MTU	The maximum size, in bytes, of any frame passing through the VC. Values can be between 64 to 65535. The service MTU must be lower than or equal to the MTU defined on all of the service's UNIs.
Core Technology	VPLS or H-VPLS. See Core Technology for Multipoint EVCs, on page 481. **Note** For VPLS or H-VPLS, you can provision a maximum number of 20 devices using the Provisioning Wizard.

Attribute	Description
VPN ID	Relevant for multipoint EVCs (both VPLS and H-VPLS). This field is automatically populated with the next available pseudowire ID. This ID can be changed during the EVC creation process (valid value range: 1-4294967295). The ID is not editable when modifying the EVC. **Note** The VPN ID is used uniquely across the network, meaning that two services will not use the same VPN ID. In addition, the VPN ID cannot use a pseudowire ID which is already configured in the network to avoid pseudowire ID collision. The VPN ID value is displayed in the PW ID field.. You cannot modify the PW ID value for multipoint services during creation and modification of services.
PW ID	Relevant for multipoint EVCs and point-to-point EVCs. This field is automatically populated with the next available pseudowire ID. You can edit this ID to assign a value only in case of point-to-point EVCs (valid value range: 1-4294967295) during the EVC creation process. The ID is not editable when modifying the EVC. **Note** The PW ID is used uniquely across the network, meaning that two services will not use the same PW ID.
Bundling	Enables multiple VLANs on this VC. Multiple CE-VLAN IDs are bundled to one EVC.
CE-VLAN ID Preservation	Ensures that the CE-VLAN ID of an egress service frame is identical in value to the CE-VLAN ID of the corresponding ingress service frame. This must be enabled if bundling is enabled.
CE-VLAN ID CoS Preservation	Ensures that the CE-VLAN CoS of an egress service frame is identical in value to the CE-VLAN CoS of the corresponding ingress service frame. The CoS markings are unaltered.

New UNI Details Reference

The following table lists and describes the attributes relating to the port that is specified as the UNI. Note that not all attributes are relevant for all the EVC types.

Table 33: New UNI Details

Attribute	Description
MTU	The Maximum Transmission Size, in bytes, of a packet passing through the interface. The MTU of the UNI must be greater than or equal to the MTU defined on the service level.
Auto Negotiation	Check this check box to automatically negotiate the speed and duplex mode.
Speed	Port speed. You can reduce the speed if this is supported on the port. **Note** This field is not available if you select the Auto Negotiation check box.
Duplex Mode	• Full Duplex—Uses simultaneous communication in both directions between the UNI and the customer's access switch, assuming that both sides support full duplex. If one side does not support full duplex, the port will be brought down. • Auto-Negotiation—Uses the mode that is agreed upon between the two devices, depending on what is supported. Full Duplex will be attempted but if one device does not support it, half duplex will be used. **Note** This field is not available if you select the Auto Negotiation check box.

Attribute	Description
Service Multiplexing	Allows the UNI to participate in more than one EVC instance.
UNI Allows Bundling	Allows the UNI to participate in VCs with Bundling enabled. See Bundling in Service Details Reference, on page 515
Untagged CE-VLAN ID	The ID of the CE-VLAN assigned to untagged traffic.
Ingress/Egress QoS Profile	Select the required QoS profile for ingress or egress traffic on the UNI. The list of profiles includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles.
UNI QoS Profile	Applies a QoS profile on the UNI itself to define the bandwidth profile and other quality of service attributes of the UNI. If you apply a QoS profile on the UNI level, you should not apply a QoS profile on the service level.
Enable Link OAM	Enables IEEE 803.1ah link operation and maintenance. If Link OAM is enabled, you will see events relating to the state of the link between this UNI and the customer's access switch.
Enable Link Management	Enables the customer access switch to get information about this UNI, VLAN IDs, services on the UNI, and so on.

UNI Service Details Reference

The following table lists and describes the attributes of the EVC in relation to the UNI, that is, how the EVC operates on this UNI. Not all attributes are relevant for all the EVC types.

Note For QinQ attributes, only the attributes that are supported on the selected device appears in the wizard.

Table 34: UNI Service Details

Attribute	Description	Additional Information
Ingress/Egress Service QoS Profile	Select the required QoS profile for ingress or egress traffic on the UNI. The list of profiles includes policy maps that were configured on the device and discovered by the system and user-defined QoS profiles.	
Layer 2 Control Protocol Profile	Profile that determines how the various communication protocols are handled. Frames using the various protocols are either tunneled, dropped, or peered. Refer to MEF 6.1 for details.	
Designation	For E-Tree: Select the role of the UNI in the VC, either Leaf or Root.	
Use point to point connection with Root	For E-Tree: If the UNI is designated as a leaf, you can select this check box to create an active pseudowire between root and leaf. The check box will not appear if there is more than one endpoint on a single device or if there is more than one root in the service.	

Attribute	Description	Additional Information
Match	Select the type of tagging the traffic should have in order to enter the UNI: • Dot1q—Mapping of 802.1q frames ingress on an interface to the service instance. • Dot1ad—Mapping of 802.1ad frames ingress on an interface to the service instance. • Default—Traffic that is not assigned to any other VC on this port. • Untagged—Frames that have no VLAN tag.	
Auto Allocate VLAN	Check this check box to automatically allocate a VLAN ID for the UNI.	
VLAN(s)	VLAN identifier, an integer 1–4094. You can enter a range of VLAN IDs using a hyphen or a comma-separated series of VLAN IDs.	This field is not available if you have checked the Auto Allocate VLAN check box.
Inner VLAN(s)	VLAN identifier for the second level of VLAN tagging, an integer 1–4094. You can enter a range of VLAN IDs using a hyphen or a comma-separated series of VLAN IDs.	
Untagged Bundled	Enables traffic with no VLAN tags to be bundled together with VLAN tagged frames.	
Priority Tagged Bundled	Enables priority tagged traffic to be bundled together with VLAN tagged frames.	
Exact	Prevents admittance of traffic with additional inner VLAN tags other than those that are matched to be carried by the service.	Applicable for IOS-XR devices only.
Outer VLAN CoS	The outer VLAN Class of Service identifier that should be associated with the frame. The CoS ID can be an integer 0–7.	Applicable for IOS devices only.
Inner VLAN CoS	The inner VLAN Class of Service identifier that should be associated with the frame. The CoS ID can be an integer 0–7.	Applicable for IOS devices only.
E-Type	Limits the service to only carry frames of the specified Ethertype: • IPv4 • IPv6 • PPPoE-All • PPPoE-Discovery • PPPoE-Session	Applicable for IOS devices only.

Attribute	Description	Additional Information
Rewrite Definition Action	The encapsulation adjustment to be performed when the frame enters the UNI: • None • Pop—Removes one or two VLAN tags from the frame on ingress and adds them on egress. • Push—Adds one or two VLAN tags from the frame on ingress and removes them on egress, either Dot1q or Dot1ad tags. • Translate—Replaces VLAN tags with new VLAN tags, either Dot1q or Dot1ad tags The translation can be 1:1, 1:2, 2:1, or 2:2.	The Translate action is applicable for IOS-XR devices only.

Service OAM

On the service level, you can define EOAM (Ethernet Operations, Administration and Management) parameters that will allow monitoring and troubleshooting of the EVC. Effectively, you will be configuring Connectivity Fault Management (CFM) components on the endpoints of the EVC.

For a point-to-point EVC, you can define OAM parameters in one direction, i.e., from UNI A to UNI Z or in both directions. For a multipoint EVC, you can define the source and destination MEP groups and then associate the EVC endpoints with a specific MEP group.

See Configure EOAM Fault and Performance Monitoring, on page 430 for more information about CFM and for device-level CFM configuration.

Use the Service OAM section in the Customer Service Details page of the Provisioning Wizard to define the specifications of the service frame to be monitored and to define the OAM profile to apply to that frame, as follows:

- From—The source of the traffic flow across the EVC.
- To—The destination of the traffic flow across the EVC.
- Direction (E-Tree only) —The direction of traffic flow between leaf and root, or root to root.

Note Your input in the From and To fields creates MEP groups, or ordered sets of UNIs. In the next page of the wizard, you will associate the UNI with one of these MEP groups.

- CoS—The Class of Service identifier that should be associated with the frame.
- OAM Profile—A set of OAM attributes that should be applied to the frame to enable performance monitoring. The following OAM profiles are available for selection:
  - Performance Monitoring 1: Enables continuity check and synthetic loss measurement. This profile supports both point-to-point and multipoint EVCs.
  - Performance Monitoring 2: Enables continuity check, synthetic loss measurement, and single-ended delay measurement. This profile supports both point-to-point and multipoint EVCs.
  - Performance Monitoring 3: Enables continuity check, synthetic loss measurement, and dual-ended delay measurement. This profile supports both point-to-point and multipoint EVCs.

- Performance Monitoring 3: Enables continuity check, synthetic loss measurement, and dual-ended delay measurement. This profile supports frame size of 64 (loss & delay) , history interval 2 (delay) and 5(loss) , aggregate interval 60.
- Performance Monitoring 4: Enables continuity check, synthetic loss measurement, and dual-ended delay measurement. This profile supports frame size of 152 (loss & delay), history interval 10, aggregate interval 300 (5 min samples) .

- Continuity Check Interval—The interval between continuity check messages.

Configure a Device and Interface To Be a UNI

The User Network Interface (UNI) is the physical demarcation point between the responsibility of the Subscriber (the Customer Edge or CE) and the responsibility of the Service Provider (the Provider Edge or PE).

UNIs demarcate the endpoints of EVCs, so configuring device interfaces as UNIs is an essential part of VC provisioning. UNI configuration can be done during the VC creation process. Alternatively, you can configure UNIs independently of VC creation. These UNIs will be available for selection during VC creation.

To configure a UNI:

Step 1 Follow the instructions in Create and Provision a New Carrier Ethernet EVC, on page 508 to access the Provisioning Wizard.

Step 2 Select **Carrier Ethernet** from the Technology drop-down list.

Step 3 Select **UNI** from the Service Types list.

Step 4 Click **Next** to go to the Customer Service Details page.

Step 5 Provide a unique name and description for the UNI, and associate it with a customer, if required.

Step 6 Define the service attributes of the UNI, as follows:

- All to One Bundling—For port-based VCs where the UNI is dedicated to the VC. When enabled, all CE-VLAN IDs are bundled to one VC. When All to One Bundling is selected, Multiplexing and Bundling cannot be selected.
- Service Multiplexing—For VLAN-based VCS where the UNI is shared between multiple VCs. When enabled, allows the UNI to participate in more than one EVC instance.
- Bundling—Allows the use of multiple VLANs for this UNI. Multiple CE-VLAN IDs are bundled to one EVC.

Step 7 Under Deploy, select whether you want to deploy the UNI immediately upon completion or first display a preview of the CLI that will be deployed to the device.

Step 8 Click **Next** to go to the UNI Details definition page.

Step 9 Select the device and port you want to configure as the UNI.

Step 10 Configure the UNI attributes, as described in New UNI Details Reference, on page 516.

Step 11 Click **Submit**. If you previously chose to deploy the circuit upon completion, a job is created and the required CLI is deployed to the devices. If you chose to see a preview of the CLI before actually deploying to the devices, the preview will be displayed now . Verify the CLI and if you want to change any of the attributes, click **Edit Attributes**. Else, click **Deploy**.

Configure a Device and Interface To Be an ENNI

The External Network to Network Interface (ENNI) specifies the reference point that is the interface between two Metro Ethernet Networks (MENs) where each operator network is under the control of a distinct administration authority. The ENNI is intended to support the extension of Ethernet services across multiple operator MENs, while preserving the characteristics of the service.

When provisioning an E-Access VC, you need to define the ENNI that will carry traffic through to the adjacent network. ENNI configuration can be done during the VC creation process. Alternatively, you can configure ENNIs independently of VC creation. These ENNIs will be available for selection during VC creation.

To configure an ENNI:

Step 1 Follow the instructions in Create and Provision a New Carrier Ethernet EVC, on page 508 to access the Provisioning Wizard.

Step 2 Select **Carrier Ethernet** from the Technology drop-down list.

Step 3 Select **ENNI** from the Service Types list.

Step 4 Click **Next** to go to the Customer Service Details page.

Step 5 Provide a unique name and description for the ENNI, and associate it with a customer/operator, if required.

Step 6 Under Deploy, select whether you want to deploy the ENNI immediately upon completion or first display a preview of the CLI that will be deployed to the device.

Step 7 Click **Next** to go to the ENNI Details definition page.

Step 8 Select the device and port(s) you want to configure as the ENNI.

Step 9 Define the following parameters for the ENNI:

- MTU—The Maximum Transmission Size, in bytes, of a packet passing through the interface. The MTU of the ENNI must be greater than 1526.
- Speed—If required, you can reduce the speed of the port if this is supported.

Step 10 Click **Submit**. If you previously chose to deploy the circuit upon completion, a job is created and the required CLI is deployed to the devices. If you chose to see a preview of the CLI before actually deploying to the devices, the preview will be displayed now. Verify the CLI and if you want to change any of the attributes, click **Edit Attributes**. Else, click **Deploy**.

Segment Routing

Configure Segment Routing

Segment Routing (SR) is a flexible, scalable way of doing source routing. The source router chooses a path, either explicit or Interior Gateway Protocol (IGP) shortest path and encodes the path in the packet header as an ordered list of segments. Segments represent subpaths that a router can combine to form a complete route to a network destination. Each segment is identified by a segment identifier (SID) that is distributed throughout the network using new IGP extensions.

Each router (node) and each link (adjacency) has an associated SID. Node segment identifiers are globally unique and represent the shortest path to a router as determined by the IGP. The network administrator allocates

a node ID from a reserved block to each router. On the other hand, an adjacency segment ID is locally significant and represents a specific adjacency, such as egress interface, to a neighboring router. Routers automatically generate adjacency identifiers outside of the reserved block of node IDs. In an MPLS network, a segment identifier is encoded as an MPLS label stack entry. Segment IDs direct the data along a specified path. A node segment can be a multi-hop path while an adjacency segment is a one-hop path.

Note SR policy visualization overlay is not supported for subinterfaces.

Create and Provision Segment Routing Policies

To create and provision SR Policies:

Before you begin

Before you provision an SR policy, ensure that the following prerequisites are met:

- MPLS TE is enabled on the device and at the router protocol level (ISIS / OSPF)
- SR-TE should be configured as the preferred option for traffic-eng
- Label allocation at the block level and for the loopback interface

Step 1 In the left plane, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Device Groups** button in the toolbar and select the group of devices you want to show on the map.

Step 3 In the Circuits/VCs tab, click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Step 4 Select **Segment Routing** in the Technology drop-down list. Cisco EPN Manager displays a list of relevant circuit/VC types in the Service Type area.

Step 5 In the Service Type list, select **SR Policy**.

Step 6 If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 7 Click **Next** to go to the Service Details page.

Step 8 (Optional) Select the customer for whom the policy is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 9 Enter the Service Details.

The service details consists of **Activate** check box, **Name**, and **Description**. Use the **Activate** check box to set the operational status of the policy to Up or Down.

Step 10 Enter the policy details. For more information, see Field References for Policy Details—SR Policy, on page 523.

Step 11 Enter the Autoroute Settings details. For more information, see Field References for Autoroute Settings Details—SR Policy, on page 523.

Step 12 In the **Deployment Action** field, specify what you want to do when the policy creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion. For more information see, Save and Schedule a Provisioning Order, on page 579.

Step 13 Click **Next** to go to the Path and Constraint Details page.

Step 14 Specify the Candidate Paths, Path Details, and Path Constraint Details. For more information, see Field References for Path and Constraint Details—SR Policy, on page 524.

Step 15 Click **Next** to go to the Template Details page. For more details on the template, see Extend a Circuit/VC Using Templates, on page 609.

Step 16 Click **Submit**. Depending on the deployment action you have chosen, the relevant action will be performed. That is, if you have chosen to preview the configuration, the preview page will be displayed where you can view the configurations, and then click **Deploy**. If you have chosen to deploy, the configurations will be directly deployed to the relevant devices.

Field References for Policy Details—SR Policy

The following table lists and describes the attributes that define the policy details for creating a Segment Routing Policy.

Table 35: Policy Details Section Reference—SR Policy

Attribute	Description
Policy Name	Enter a policy name.
Head End	Select the head end from the drop down list.
Color	The color value range is from 1 to 4294967295.
End Point	Select the end point from the drop down list.
Explicit Binding SID	The Explicit Binding SID range is from 16 to 1048575.
Bandwidth	The bandwidth value range depends on the value selected in the **Bandwidth Unit** field.
Bandwidth Unit	Choose a value from the drop-down list. The available options are **Kbps**, **Mbps**, and **Gbps**.

Note The **Bandwidth** and **Bandwidth Unit** field is only applicable for **Dynamic With PCE** path type.

Field References for Autoroute Settings Details—SR Policy

The following table lists and describes the attributes that define the Autoroute Settings details for creating a Segment Routing Policy.

Table 36: Autoroute Settings Details Section Reference—SR Policy

Attribute	Description
Auto Metric Mode	Select a value from the drop down list. The available options are **Constant** and **Relative**.
Auto Metric Value	Depending on the value selected in the Auto Metric Mode field, the range of the Auto Metric Value changes. For Constant the range is from 1 to 2147483647. For Relative the range is from -10 to 10.

Attribute	Description
Allow All Prefixes	Select the check box if you want to allow all IP prefixes.
Allowed Prefixes	This field only appears if the Allow All Prefixes check box is not selected. Add the required prefixes to the table.

Field References for Path and Constraint Details—SR Policy

The following table lists and describes the attributes that define the path constraint details for creating a Segment Routing Policy.

Table 37: Path Constraint Details Section Reference—SR Policy

Attribute	Description
Candidate Paths	
Path Type	Choose the required path for the SR Policy. The values are **Dynamic**, **Explicit**, and **Dynamic With PCE**.
Preference	The candidate path preference value ranges from 1 to 65535.
Path Details for Dynamic and Dynamic With PCE path type:	
Metric Type	Choose the required Metric Type. The values are **IGP**, **Latency**, **TE**, and **HopCount**.
Metric Margin Type	Choose the required Metric Margin Type. The values are **Absolute** and **Relative**.
Metric Margin Value	The Metric Margin Value range is from 0 to 2147483647.
Max SID Limit	The Max SID Limit is from 1 to 255.
Path Details for Explicit path type:	
New Segment List	Select the check box if you want to create a new segment list.
Segment List Name	This filed appears if New Segment List check box is selected.
Existing Segment List	This field appears if the New Segment List check box is not selected. Select a segment list from the drop down list.
Weight	The weight range is from 1 to 4294967295.

Note When entering the path details, you must click the **+** icon and provide the **Segment List Name** and **Weight** to add details to the Segment list.

The Segments table is active for editing if the New Segment List check box is selected.

- You can add Segment by clicking +. Provide the **Index** value and select the **Device**, **Segment Type**, and **Interface**from the respective drop down lists.
- If you have added multiple segments, you can place them in your desired queue by using the up or down arrow in the segments window.
- You can also edit or delete a segment from the segments window only when you are creating it. Once the segment list is created, it cannot be modified.
- You can also assign label for the interfaces which do not have label assigned to them.

Attribute	Description
Path Constraint Details	
Affinity Operation	Individually select the applicable affinity operations and specify the related details. The values are **Exclude-Any**, **Include-Any**, and **Include-All**.
Exclude Any Affinity Names	Select the names from the drop-down list.
Include Any Affinity Names	This field appears if **Include-Any** is selected. Select the affinity name that you want to include from the drop down list.
Include All Affinity Names	This field appears if **Include-All** is selected. Select the affinity name that you want to include from the drop down list.
SID Algorithm	The SID Algorithm range is from 128 to 255.
Disjoint Group Type	Select a value from the drop-down list. The value are **Link**,**Node**, **Srlg**, and **Srlg-Node**.
Disjoint Group Id	The Disjoint Group Id range is from 1 to 65535.
Disjoint Sub Group Id	The Disjoint Sub Group Id range is from 1 to 65535.

Create and Provision Carrier Ethernet Services with Segment Routing Policies

The Cisco EPN Manager supports provisioning of EPL, EVPL, Access EPL, Access EVPL carrier ethernet point-to-point services using Segment Routing traffic engineering(SR-TE) policy. You can modify SR-TE policy during modification of CE services. Related Circuits/VCs tab in Circuit/VCs 360* can be used to view the SR policies associated to this service. For SR-policy, the backup path visualization is available in the overlay. You can expand the **Show Backup Path** and choose the nodes or links that you want to exclude. When you click **Apply**, the new backup path is displayed.

To create and Provision an EVPL Service with SR Policies:

Step 1 In the left plane, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the Device Groups button in the toolbar and select the group of devices you want to show on the map.

Step 3 In the Circuits/VCs tab, click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Step 4 Select **Carrier Ethernet** in the Technology drop-down list. Cisco EPN Manager displays a list of relevant circuit/VC types in the Service Type area. For example, Carrier Ethernet service types include EPL, EVPL, EP-LAN, and so on.

Step 5 In the Service Type list, select the type of circuit/VC you want to create. For example, EVPL.

Step 6 If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 7 Click **Next** to go to the Service Details page.

Step 8 (Optional) Select the customer for whom the EVPL is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 9 Enter the Service Details. See Service Details Reference, on page 515 for descriptions of the fields and attributes.

Step 10 Click **Next**.

Step 11 In the **Deployment Action** field, specify what you want to do when the EVPL creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment

or you can deploy the configurations immediately upon completion. For more information see, Save and Schedule a Provisioning Order, on page 579.

Step 12 Click **Next** to go to the page(s) in which you define the UNI(s). In the case of E-Access, there is an additional page for defining the ENNI.

Step 13 Identify the device and interface that will serve as the UNI:

Note If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, select the Unmanaged check box and provide information for the unmanaged device. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 609

Step 14 If you are creating a new UNI, enter the New UNI Details. See New UNI Details Reference, on page 516 for descriptions of the fields and attributes.

Step 15 Enter the UNI Service Details. See UNI Service Details Reference, on page 517 for descriptions of the fields and attributes.

Step 16 If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, select the **Unmanaged** check box and provide information for the unmanaged device. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 609 for more information.

Step 17 For E-LAN and E-TREE EVCs with H-VPLS as the core technology, select the devices that will serve as the primary and secondary hubs.

Step 18 For E-Line and E-Access EVCs: In the Pseudowire Settings page, you can select SR-TE policy for segment routing over which the EVC will traverse, as follows:

a. Check the **Static Preferred Path** check box to assign a static route for the service.

Note For E-access this check box is not applicable.

b. Click the **SR Policy** radio button.

c. Select the required SR-TE policy from the Preferred Path (A-Z) and Preferred Path (Z-A) drop-down lists.

Note Both Preferred Path(A-Z) and Preferred Path(Z-A) are optional fields.

d. Repeat steps 5 through 8 in Create and Provision a New Carrier Ethernet EVC, on page 508.

Step 19 Repeat steps 20 through 22 Create and Provision a New Carrier Ethernet EVC, on page 508.

Provision Circuits in an Optical/DWDM Network

- Create and Provision an OTN Circuit, on page 544
- Create and Provision an ODU Circuit, on page 549

Summary of Cisco EPN Manager Optical/DWDM Network Provisioning Support

Cisco EPN Manager supports the provisioning of Dense Wavelength Division Multiplexing (DWDM) optical channel (OCH) circuit types. The DWDM optical technology is used to increase bandwidth over existing fiber optic backbones. It combines and transmits multiple signals simultaneously at different wavelengths on the same fiber. In effect, one fiber is transformed into multiple virtual fibers.

Cisco EPN Manager supports the following optical circuits:

- Dense Wavelength Division Multiplexing (DWDM) optical channel (OCH) circuit—Following are the different optical channel circuit types:
  - Optical Channel Network Connection (OCHNC) WSON—OCHNC WSON circuits establish connectivity between two optical nodes on a specified C-band wavelength. For more information, see Optical Channel Network Connection (OCHNC) WSON, on page 486.
  - Optical Channel Client Connection (OCHCC) WSON—OCHCC WSON circuits extend the OCHNC WSON to create an optical connection from the source client port to the destination client port of the TXP/MXP cards. For more information, see Optical Channel Client Connection (OCHCC) WSON, on page 486.
  - Optical Channel (OCH) Trail WSON— OCH trail WSON circuits transport the OCHCC WSON circuits. For more information, see Optical Channel (OCH) Trail WSON, on page 487.
  - Optical Channel (OCH) Trail connecting NCS 1002, NCS 55xx, and ASR 9K devices—This OCH trail circuit creates an optical connection from the source trunk port of an NCS 1002, NCS 55xx, or ASR 9K device to the destination trunk port of another similar device. For more information, see Optical Channel (OCH) Trail Connecting NCS 1002, NCS 55xx, and ASR 9K Devices, on page 488.
  - Optical Channel (OCH) Trail User-to-Network Interface (UNI)—An OCH trail UNI circuit establishes connectivity between Cisco NCS 2000 series devices and Cisco NCS 4000 series devices. For more information, see Optical Channel (OCH) Trail User-to-Network Interface (UNI), on page 488.
  - Spectrum Switched Optical Network (SSON)—SSON circuits allow you to provide more channels in a span. Using the SSON functionality, the circuits are placed closer to each other if they are created within a media channel group. For more information, see Spectrum Switched Optical Network (SSON) Circuits, on page 489.
- Optical Transport Network (OTN)—An OTN circuit can be established statically or dynamically between ingress and egress nodes using Resource Reservation Protocol (RSVP) signaling. For more information, see Optical Transport Network (OTN) Circuit, on page 490.
  - Optical Channel Data Unit User-to-Network Interface (ODU UNI)—An ODU UNI circuit represents the actual end-to-end client service passing through the OTN architecture. For more information, see Optical Channel Data Unit User-to-Network Interface (ODU UNI), on page 490.
  - Optical Channel Data Unit (ODU) Tunnel—ODU tunnel circuits transport the ODU UNIs. For more information, see Optical Channel Data Unit (ODU) Tunnel, on page 491.

- Optical Channel Payload Unit (OPU) Over Optical Channel Data Unit (ODU)—OPU over ODU circuits provide a high-bandwidth point-to-point connection between two customer designated premises.These circuits uses ODU UNI circuits to carry client signals through the network. For more information, see Optical Channel Payload Unit (OPU) Over Optical Channel Data Unit (ODU), on page 491.
- Optical Channel Data Unit User-to-Network Interface (ODU UNI) Hairpin—An ODU UNI Hairpin circuit is similar to an ODU UNI circuit, but it is created in the management plane and it is an intra node circuit, that is, the source and destination is the same device but with different interfaces. For more information, see Optical Channel Data Unit User-to-Network Interface (ODU UNI) Hairpin, on page 492.
- Optical Channel Data Unit (ODU)—Optical Channel Data Unit (ODU) is created as a sub controller of an OTU controller. ODU contains information for the maintenance and operational functions to support optical channels. For more information, see Optical Channel Data Unit (ODU), on page 492.

Prerequisites for Provisioning Optical Circuits

Following are the prerequisites for provisioning an optical circuit:

- Cisco EPN Manager supports both, Wavelength Switched Optical Network (WSON) and non-WSON circuits. However, for non-WSON circuits, Cisco EPN Manager supports only circuit discovery, which includes circuit overlay, circuit 360 view, multilayer trace view, and circuit details. Cisco EPN Manager does not support the provisioning, activation, deactivation, protection switch actions, and modification of non-WSON circuits.
- Communication between devices must be set up before you can provision an optical circuit.
- Inventory collection status for the devices on which the optical circuits will be provisioned must be *Completed*. To check this, go to **Inventory** > **Device Management** > **Network Devices**, and look at the status in the **Last Inventory Collection Status** column.
- DWDM grid unit must be set to either, wavelength or frequency. To do this, go to **Administration** > **Settings** > **System Settings** > **Circuits/VCs Display**, and under the DWDM Grid Unit area, choose either **Wavelength (Nanometer (nm))** or **Frequency (Terahertz (THz))**.
- Before you provision an OCHNC or a Media Channel NC circuit using NCS 2000 series devices running on software version 10.7 or later, ensure that you create a UNI config, either in Cisco Transport Controller (CTC) or in Cisco EPN Manager.
- Optionally, customers must be created in the system so that you can associate a circuit/VC to a customer during the circuit/VC creation and provisioning process. From the left sidebar, choose **Inventory** > **Other** > **Customers** to create and manage customers.
- For NC57-18DD-SE cards, use the following command format to reuse the ports 0-17 and 24-29 in 400G mode:

  `hw-module port-range <start port> <end port> location <loc> mode <port_mode>`

  Example: **`hw-module port-range 8 9 location 0/1/CPU0 mode 400`**

Create and Provision an OCH Circuit

To provision an OCH circuit, carry out these steps:

Before you begin

For information about the prerequisites before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 528.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and select the location in which you want to create the OCH circuit.

Step 3 Close the **Device Groups** pop-up window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

(You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.)

Step 6 From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, Optical service types for OCH circuits include OCHNC, OCHCC, OCH-Trail, OCHNC WSON, OCHCC WSON, OCH-Trail WSON, and OCH-Trail UNI.

Step 7 In the **Service Type** area, choose the type of OCH circuit you want to create.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the **Customer Section** page.

Step 10 (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 11 Enter the circuit name and its description in the **Customer Section** page.

Step 12 Click **Next** to go to the **Circuit Section** page.

Note If you select OCH-Trail UNI as the optical service type, the **Endpoint Section** page appears first, followed by the **Circuit Section** page.

Step 13 Enter the circuit details. See Circuit Section Reference for OCH Circuit Types, on page 531 for descriptions of the fields and attributes.

Step 14 Click **Next** to go to the **Endpoint Section** page.

Step 15 Select the bandwidth from the **Bandwidth** drop-down list.

Step 16 Select a row in the Endpoint table, and click a device in the map to populate the Device Name column with the selected device. You can also click the row in the Endpoint table to edit the Device Name, Termination Point, Add/Drop Port, OCH-Trail, and Side columns. The Side column gets auto-populated based on the port selected. Only network elements that are available and compatible with the circuit type you chose is displayed.

Select the endpoints with the same FEC modes. If you select endpoints with different FEC modes, an error message is displayed.

Note The **Add Port** and **Drop Port** columns are available only for OCHNC WSON circuit. When you choose the port that must be added to the Add Port column, the values in the Drop Port and Side columns get auto populated. Also, you can manually edit the values in the Drop Port column.

Step 17 Select a trail diversity for the OCH circuit. The OCH circuit that you are creating is diverse from the trail that you choose.

Note You cannot modify or delete the created trail diversity.

For OCHNC circuits you can select the **Diversity for PSM** check box and add the diversity.

Step 18 Click **Next** to go to the **Constraints Section** page.

Step 19 Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table toolbar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the chosen circuit type are displayed.

Note When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table. The following route constraint conditions apply to the OCHCC Trail WSON circuit:

- The modified route constraints are not applied immediately to the circuit but might cause a reroute. However, the modification is applied at the next route operation or restoration.
- The **Circuit Overlay** shows only the constraints applicable to current route, while the **Circuit Edit** wizard displays the currently configured constraints.
- The **Circuit Edit** wizard contains the constraints table displaying the different constraints with respect to constraints icon displayed using circuit overlay.
- While modifying the circuit, you can select the **Reroute Actions** from the drop-down list. You can select None, Working Path, or Protection path from the list.
- To include or exclude the associated OTS link in a working path, select the Source link termination point while selecting the OTS link termination point with the optical degree as a constraint. For example, consider a three-node topology, where all the three nodes (A, B, and C) are connected, and the circuit has A and B as a Source Node and Destination Node, respectively. If you want to include a working path link that connects B and C, then while selecting the constraint, select the link termination point listed with the optical degree that connects to C. For example, if optical degree 1 of node B is used to connect C, select constraint as B-1. This scenario is applicable for including or excluding the link in a working path.

Step 20 Click **Next** to go to the **Alien Wavelength Section** page. The current Alien Wavelength configurations such as the Card, Trunk mode, and FEC mode for the source and destination nodes are displayed. You can choose to create new configurations of the Alien Wavelength for the source and destination nodes.

Note The **Alien Wavelength Section** is available only when you create OCHNC WSON circuits.

Step 21 Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that are deployed to the devices, it is displayed on clicking **Preview**. You can either deploy the configurations to the device or cancel it but you cannot edit the attributes.

Note If you get an error message stating "Cannot validate the activation of the circuit. Time out expired ", it means that device is taking time to activate the circuit in control plane. The circuit is in missing state in EPNM. Deleting it on EPNM does not delete the circuit on the network. Device full synchronization from EPNM must be done if the circuit has to be shown as UP & discovered in EPNM. It has to be deleted from CTC so that it can be created again from EPNM.

Step 22 The circuit is added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Note If only an OCH-Trail is created, the Related Circuits tab in Circuit/VC 360 does not show any data. If an OCHCC is created, it also creates an OCH-Trail. For these circuits, in the Related Circuits tab OCHCC-WSON contains OCH-Trail WSON and OCH-Trail WSON contains OCHCC-WSON.

Circuit Section Reference for OCH Circuit Types

Table 38: Circuit Section Reference—OCH Circuit Types

Attribute	Description	Enabled
Circuit Details		
Label	Unique name to identify the circuit.	
State	Administrative state for the circuit. Values are: • In Service—The circuit is in service and able to carry traffic. • Out of Service—The circuit is out of service and unable to carry traffic.	For all OCH circuit types.
Bidirectional	Check this check box to create a two-way circuit.	For OCHCC WSON and OCH Trail WSON circuit types.
Wait For Activation	Check this check box to wait for the set time for circuit activation.	For OCHCC WSON and OCH Trail WSON circuit types.
Protection	Protection mechanism for the circuit. Cisco EPN Manager supports the following protection mechanism based on the circuit type selected: • None—For unprotected circuits This value is available for all OCH circuit types. • PSM—When a Protection Switch Module (PSM) card is connected to a TXP card. This value is available for OCHNC WSON and OCHCC WSON circuit types. • Y-Cable—When a transponder or muxponder card protects the circuit. This value is available for OCHCC WSON circuit type. • Splitter—When a MXPP/TXPP card is used. The circuit source and destination are on MXPP_MR_2.5G and TXPP_MR_2.5G cards. These cards provide splitter (line-level) protection (trunk protection typically on TXPP or MXPP transponder cards). This value is available only for OCHCC WSON circuit type.	For OCHNC WSON circuit type.

Attribute	Description	Enabled
Route Properties		
Diverse From Tunnel	Select a tunnel to ensure that it is not used by the circuit you are provisioning. This is to ensure that if there is a failure in a tunnel, the same tunnel is not used by another circuit.	For OCH-Trail UNI circuit types when the Mutual Diversity check box is unchecked.
Validation	Validation mode for the circuit. Values are: • Full—The circuit is created when the circuit validation result is greater than or equal to the acceptance threshold value. • None—The circuit is created without considering the acceptance threshold value.	For all OCH circuit types.
Acceptance Threshold	Protection acceptance threshold value set for the OCH protected circuits. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For all OCH circuit types when the Validation field is set to Full.
Protect Acceptance Threshold	Protection acceptance threshold value set for the OCH protected circuits. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For OCHNC WSON circuit type when: • Protection field is set to PSM, Y-Cable, or Splitter. • Validation field is set to Full.
Ignore Path Alarms	Check the check box to ignore path alarms.	For OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types.
Allow Regeneration	Check the check box to allow the network elements to regenerate the signal.	For all OCH circuit types.

Attribute	Description	Enabled
Soak Time	Period that the circuit on the restored path waits before switching to the original path after a failure is fixed.	For OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types when Revert is set to Manual or Automatic.
Restoration	Check this check box to restore the failed OCH circuit to a new route.	For all OCH circuit types.
Restoration Frequency	Select the restoration frequency type by checking the **Preferred** or **Required** radio button.	For OCH-Trail circuit type when the Restoration check box is checked.
Priority	Prioritize the restoration operation for the failed OCH circuit. Values are High, Priority 1, Priority 2, Priority 3, Priority 4, Priority 5, Priority 6, and Low.	For all OCH circuit types when the Restoration check box is checked.
Restoration Validation	Validation mode for the restoration operation. Values are: • None—The circuit is restored without considering the restoration acceptance threshold value. • Inherited—The restoration circuit inherits the validation and acceptance threshold values from the primary circuit. • Full—The circuit is restored when the restoration validation result is greater than or equal to the restoration acceptance threshold value.	For all OCH circuit types when the Restoration check box is checked.
Restoration Acceptance Threshold	Acceptance threshold value set for the restoration operation for OCH circuits. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For all OCH circuit types when: • Restoration check box is checked. • Restoration Validation field is set to Full.

Attribute	Description	Enabled
Restoration Protect Acceptance Threshold	Protection acceptance threshold value set for the restoration operation for OCH protected circuits. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For OCHNC WSON circuit type when: • Protection field is set to PSM, Y-Cable, or Splitter. • Restoration check box is checked. • Restoration Validation field is set to Full.
Restoration Soak Time	Period that the circuit on the optical path waits before restoring to a new path after a failure alarm is raised. The default restoration soak time is 2 minutes.	For OCH-Trail and OCH-NC, when Restoration is selected.
Revert	Reverts the circuit from the restored path to the original path after a failure is fixed. Values are None, Manual, and Automatic.	For OCHCC WSON, OCHNC WSON, OCH-Trail and OCH-Trail WSON circuit types when the Restoration check box is checked.
Revert Soak Time	Period that the circuit on the optical path waits before reverting to the original path after a failure is fixed. The default revert soak time is 1 minute.	For OCH-Trail and OCH-NC, when Revert is set to Automatic.
Admin State	Select the admin state of the circuit as **Up** or **Down**. This impacts the circuit's operability and determines whether the circuit can be activated or deactivated.	For OCH-Trail UNI circuit type.
Optical Properties		
Grid Type	Choose the desired grid type from the drop-down list. You can choose from **Flex 6.25 GHz**, **Fixed 50 GHz**, **Flex 100 MHz**, and **Fixed 75 GHz**.	For OCH-Trail circuit type.
Wavelength (nm)/ Frequency (THz)	Choose the wavelength from the drop-down list.	For OCH-Trail circuit type.
Main Frequency	Select the frequency type by clicking the **Preferred** or **Required** radio button.	For OCH-Trail circuit type.
Preferred Wavelength Properties		
Wavelength Options	Wavelength options for the circuit. Values are **Do Not Set**, **Set To Default**, and **Set Preferred Wavelength**.	For OCH-Trail UNI circuit type.

Attribute	Description	Enabled
Work Port Properties		
Auto Provisioning	Check this check box to enable the Auto Provisioning feature.	For all OCH circuit types
C Band	Conventional wavelength window to provision the circuit. Values are: • Odd—The odd position in the ITU grid. • Even—The even position in the ITU grid.	• For all OCHCC WSON, OCHNC WSON, and OCH-Trail WSON circuit types when the Auto Provisioning check box is unchecked. • • In Service—The circuit is in service and able to carry traffic. • Out of Service—The circuit is out of service and unable to carry traffic.
Wavelength/Frequency	Wavelength or frequency of the circuit. This value is applicable for the C Band that you chose. **Note** You must set the DWDM grid unit to either wavelength or frequency. To do this, go to **Administration** > **Settings** > **System Settings** > **Circuits/VCs Display**, and under the DWDM Grid Unit area, choose either **Wavelength (Nanometer (nm))** or **Frequency (Terahertz (THz))**.	For all OCH circuit types when the C Band field is set to Odd or Even.
Preferred/Required	Select to determine whether the values set in the C Band and Wavelength/Frequency fields are preferred or required to provision the circuit.	For all OCH circuit types when the Auto Provisioning check box is unchecked.
Protect Port Properties		

Attribute	Description	Enabled
Copy from Work Port	Check this check box to copy the values set in the Work Port Properties section.	For all OCH circuit types when the Protection field is set to PSM, Y-Cable, or Splitter.

Note EPNM supports the following parameters for legacy circuit color validation while creation OCH-Trail:

- AmpliGainRange
- ChPwr
- Gain
- Tilt
- WkgMode - OpticalAmplificationSettings tableVoaAttenuation
- Attenuator - OpticalTransportSettings table

Reactive inventory will not get triggered if these port parameters changed on the device. You have to trigger sync operation to get the parameters updated in EPNM.

Create and Provision an OCH Trail Circuit Connecting IOS-XR Platform Based Devices Directly

To create and provision an OCH trail circuit connecting the IOS-XR platform based devices directly:

Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 528.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which you want to create the OCH circuit.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, Optical service types for OCH circuits include OCHNC WSON, OCHCC WSON, OCH-Trail WSON, and OCH-Trail UNI.

Step 7 In the **Service Type** area, choose the type of OCH circuit you want to create.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the **Customer Section** page.

Step 10 (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 11 Enter the circuit name and its description in the **Customer Section** page.

Step 12 Click **Next** to go to the **Circuit Section** page.

Note If you select OCH-Trail UNI as the optical service type, the **Endpoint Section** page appears first followed by the **Circuit Section** page.

Step 13 Enter the circuit details. See Circuit Section Reference for OCH Circuit Types, on page 531 for descriptions of the fields and attributes.

Step 14 Click **Next** to go to the **Endpoint Section** page.

Step 15 Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name, Termination Point, Add/Drop Port, OCH-Trail, and Side columns. The Side column gets auto-populated based on the port selected. Only network elements that are available and compatible with the circuit type you chose will be displayed.

Note The **Add Port** and **Drop Port** columns are available only for OCHNC WSON circuit. Once you choose the port that needs to be added to the Add Port column, the values in the Drop Port and Side columns get auto-populated. Also, you can manually edit the values in the Drop Port column.

Step 16 Select a trail diversity for the OCH circuit. The OCH circuit that you are creating will be diverse from the trail that you choose.

Note You cannot modify or delete the trail diversity once it is created.

Step 17 Click **Next** to go to the **Constraints Section** page.

Step 18 Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

Note When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table. The following route constraint conditions apply to the OCHCC Trail WSON circuit:

- The modified route constraints are not applied immediately to the circuit but might cause a reroute. However, the modification is applied at the next route operation or restoration.
- The **Circuit Overlay** shows only the constraints applicable to current route, while the **Circuit Edit** wizard will display the currently configured constraints.
- The **Circuit Edit** wizard contains the constraints table displaying the different constraints with respect to constraints icon displayed using circuit overlay.

Step 19 Click **Next** to go to the **Alien Wavelength Section** page. The current Alien Wavelength configurations such as the Card, Trunk mode, and Fec mode for the source and destination nodes are displayed. You can choose to create new configurations of the Alien Wavelength for the source and destination nodes.

Note The **Alien Wavelength Section** is available only when you create OCHNC WSON circuits.

Step 20 Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it but you cannot edit the attributes.

Step 21 The circuit should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Create and Provision Two Mutually Diverse OCH-Trail UNI Circuits

Use this procedure to create two OCH-Trail UNI circuits that are mutually diverse from each other. Both the circuits must originate from the same device. You can create both the circuits quickly using the Provisioning wizard in a single workflow .

Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 528.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which you want to create the OCH circuit.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Optical**.

Step 7 In the **Service Type** area, choose **OCH-Trail UNI**.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the **Customer Section** page.

Step 10 Check the **Mutual Diversity** check box to create two OCH-Trail UNI circuits that are mutually diverse from each other.

Step 11 Enter the circuit name and its description in the **Customer Section** page.

Step 12 Click **Next** to go to the **Endpoint Section** page.

Step 13 Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Interface.

Note When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column.

Step 14 Click **Next** to go to the **Circuit Section** page.

Step 15 Enter the circuit details. See Circuit Section Reference for OCH Circuit Types, on page 531 for descriptions of the fields and attributes.

Step 16 Click **Next** to go to the **Constraints Section** page.

Step 17 Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

Note When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

Step 18 Click **Next**. The **Customer Section** page for the second circuit is displayed.

Step 19 Repeat Step 11 to Step 17 to create the second circuit.

Step 20 Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it but you cannot edit the attributes.

Step 21 The circuits should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC names to see the Circuit/VC 360 view.

Create and Provision a Media Channel Group SSON Circuit

To create and provision a Media Channel Group SSON circuit:

Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 528.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which you want to create the Media Channel Group SSON circuit.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area.

Step 7 In the **Service Type** area, choose **Media Channel Group SSON**.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the **Customer Section** page.

Step 10 (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 11 Enter the circuit name and its description in the **Customer Section** page.

Note A maximum of only 80 characters are allowed for the Circuit Name field.

Step 12 Click **Next** to go to the **Endpoint Section** page.

Step 13 Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name, Termination Point, and Add/Drop Port columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.

Note When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column.

Step 14 Click **Next** to go to the **Circuit Section** page.

Step 15 Choose the required circuit width.

Step 16 To set the **Central Wavelength/Frequency Properties**, do one of the following:

- Check the **Auto Provisioning** check box.
- Choose the required **Wavelength** for the circuit and then choose either **Preferred** or **Required** option to determine whether the values set in the **Wavelength** field is preferred or required to provision the circuit.

Step 17 Click **Next** to go to the **Constraints Section** page.

Step 18 Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table tool bar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the circuit type you chose will be displayed.

Note When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

The **Alternate Constraints** check-box is available for selection if the **Restoration** check-box is selected and the **Revert** is set to **None** in the **Optical Properties**.

Step 19 Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview** and now, you can either deploy the configurations to the device or cancel it, but you cannot edit the attributes.

The circuit should be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Create and Provision a Media Channel SSON Circuit

To create and provision a Media Channel SSON circuit:

Before you begin

- Ensure that a Media channel group SSON is already created to associate the Media Channel SSON circuits with the Media channel group. See Create and Provision a Media Channel Group SSON Circuit, on page 539.
- For information about the prerequisites that must be met before provisioning an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 528.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and select the location where you want to create the Media Channel SSON circuit.

Step 3 Close the **Device Groups** pop-up window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the **Circuits/VCs** tab, and click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, optical service types for Media Channel SSON circuits include Media Channel NC SSON, Media Channel Trail SSON, and Media Channel CC SSON.

Step 7 In the **Service Type** area, choose the type of Media Channel SSON circuit you want to create.

Step 8 If you have defined the profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the **Customer Section** page.

Step 10 (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 11 Enter the circuit name and description in the **Customer Section** page.

Note For the Media Channel NC SSON and Media Channel Trail SSON circuits, a maximum of 77 characters are allowed in the Circuit Name field. Out of the 77 characters, three characters are reserved for the carrier suffix.

For the Media Channel CC SSON circuits, a maximum of 71 characters are allowed in the Circuit Name field.

Step 12 Click **Next** to go to the **Endpoint Section** page.

Step 13 Select a row in the Endpoint table, and click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Termination Point columns. The Side column gets autopopulated based on the termination point. Only network elements that are available and compatible with the chosen circuit type will be displayed.

Note The MCH-Trail Name column is available only when you create a Media Channel CC SSON circuit.

Step 14 Select a media channel diversity for the MCH circuit. The MCH circuit that you are creating will be diverse from the media channel that you choose.

Note You cannot modify or delete the media channel diversity once it is created.

Step 15 Click **Next** to go to the **Circuit Section** page.

Note For the Media Channel CC SSON circuits, the **Circuit Section** page is not available if you have entered an MCH-Trail Name in the Endpoints table.

Step 16 Choose the Media Channel Group that you want to associate the Media Channel SSON circuit with.

Step 17 Enter the circuit details. See Circuit Section Reference for Media Channel SSON Circuit Types, on page 542 for descriptions of the fields and attributes.

Step 18 Click **Next** to go to the **Constraints Section** page.

Note For MCHNC SSON circuits, you can add NCS1K and NCS2K devices in Regen mode as constraints.

Step 19 Click a device node or a link in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table toolbar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements and links that are compatible with the chosen circuit type will be displayed.

Note When the row is in the edit mode, you cannot click a device or a link in the map to populate the columns in the Constraints table.

Step 20 Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, click **Preview**. You can either deploy the configurations to the device or cancel it, but you cannot edit the attributes.

The circuit will be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Circuit Section Reference for Media Channel SSON Circuit Types

The following table lists and describes the attributes that define the Media Channel SSON circuit types.

Table 39: Circuit Section Reference—Media Channel SSON Circuit Types

Attribute	Description	Enabled
Central Wavelength/Frequency Properties		
Auto Provisioning	Check this check box to automatically set the wavelength or frequency properties for the circuit.	For all Media Channel SSON circuit types.
Wavelength (nm)	Wavelength or frequency of the circuit. **Note** You must set the DWDM grid unit to either wavelength or frequency. To do this, go to **Administration** > **Settings** > **System Settings** > **Circuits/VCs Display**, and under the DWDM Grid Unit area, choose either **Wavelength (Nanometer (nm))** or **Frequency (Terahertz (THz))**.	For all Media Channel SSON circuit types when the Auto Provisioning check box is unchecked.
Preferred/Required	Select to determine whether the values set in the Wavelength field is preferred or required to provision the circuit.	For all Media Channel SSON circuit types when the Auto Provisioning check box is unchecked.
Optical Properties		
Validation	Validation mode for the circuit. Values are: • Full—The circuit is created when the circuit validation result is greater than or equal to the acceptance threshold value. • None—The circuit is created without considering the acceptance threshold value.	For all Media Channel SSON circuit types.

Attribute	Description	Enabled
Acceptance Threshold	Protection acceptance threshold value set for the circuit. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For all Media Channel SSON circuit types when the Validation field is set to Full.
Ignore Path Alarms	Check the check box to ignore path alarms.	For all Media Channel SSON circuit types.
Allow Regeneration	Check the check box to allow the network elements to regenerate the signal.	For all Media Channel SSON circuit types.
Restoration	Check this check box to restore the failed Media Channel SSON circuit to a new route.	For all Media Channel SSON circuit types.
Priority	Prioritize the restoration operation for the failed circuit. Values are High, Priority 1, Priority 2, Priority 3, Priority 4, Priority 5, Priority 6, and Low.	For all Media Channel SSON circuit types when the Restoration check box is checked.
Restoration Validation	Validation mode for the restoration operation. Values are: • None—The circuit is restored without considering the restoration acceptance threshold value. • Inherited— The restored circuit inherits the validation and acceptance threshold values from the primary circuit. • Full—The circuit is restored when the restoration validation result is greater than or equal to the restoration acceptance threshold value.	For all Media Channel SSON circuit types when the Restoration check box is checked.
Restoration Acceptance Threshold	Acceptance threshold value set for the restoration operation for the circuit. Values are: • Green—Indicates that the restoration failure risk is 0%. • Yellow—Indicates that the restoration failure risk is between 0% and 16%. • Orange—Indicates that the restoration failure risk is between 16% and 50%. • Red—Indicates that the restoration failure risk is greater that 50%.	For all Media Channel SSON circuit types when: • Restoration check box is checked. • Restoration Validation field is set to Full.
Revert	Reverts the circuit from the restored path to the original path after a failure is fixed. Values are None, Manual, and Automatic.	For all Media Channel SSON circuit types when the Restoration check box is checked.

Attribute	Description	Enabled
Soak Time	Period that the circuit on the restored path waits before switching to the original path after a failure is fixed.	For all Media Channel SSON circuit types when the Revert option is set to Manual or Automatic.

Create and Provision an OTN Circuit

To provision an OTN circuit:

Before you begin

For information about the prerequisites that must be met before you can provision an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 528.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which you want to create the OTN circuit.

Step 3 In the **Network Topology** window, click **Circuits/VCs**.

Step 4 Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 5 From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area. For example, service types for OTN circuits include ODU UNI, ODU Tunnel, OPU over ODU, and ODU UNI Hairpin.

Step 6 In the **Service Type** area, choose the type of OTN circuit you want to create.

Step 7 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 8 Click **Next** to go to the **Customer Details** page.

Step 9 (Optional) Select the customer for whom the circuit is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 10 Enter the circuit name and its description in the **Customer Details** page.

Step 11 Click **Next** to go to the **Circuit Details** page.

Step 12 Enter the circuit details. See Circuit Section Reference for OTN Circuit Types, on page 545 for descriptions of the fields and attributes.

Step 13 Click **Next** to go to the **Endpoint Section** page.

Step 14 Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Interface/Termination Point columns. Only network elements that are available and compatible with the circuit type you chose will be displayed.

Note When the row is in the edit mode, you cannot click a device in the map to populate the Device Name column.

Step 15 Enter the protection type and path options for the circuit. See Endpoint Section Reference for OTN Circuit Types, on page 546 for descriptions of the fields and attributes.

Step 16 Click **Create Now** to create the circuit. If you chose to see a preview of the TL1 or CLI commands that will be deployed to the devices, it will be displayed on clicking **Preview**. After seeing the preview of the TL1 or CLI commands, you can either deploy the configurations to the devices or cancel the provisioning operation.

The circuit should be added to the list in the **Circuits/VCs** tab in the **Network Topology** window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Circuit Section Reference for OTN Circuit Types

The following table lists and describes the attributes that define the OTN circuit types.

Table 40: Circuit Section Reference—OTN Circuit Types

Attribute	Description	Enabled
Circuit Properties		
Bandwidth	Bandwidth required to provision the OTN circuit. See Table 42: Value Mapping—Bandwidth and Service Type for ODU UNI Circuits for the mapping of values in the Bandwidth, and Service Type fields.	For all OTN circuit types.
A-End Open Ended	Check this check box to create an open-ended circuit, in which the source end point is connected to an ODU subcontroller, instead of a client payload controller. **Note** Checking this checkbox will not deploy ODU subcontrollers on the Cisco NCS 4000 devices. You must configure the ODU subcontrollers on the Cisco NCS 4000 devices before adding the devices to Cisco EPN Manager. For more information about the open ended ODU UNIs and how to configure ODU subcontrollers on Cisco NCS 4000 devices, see Open Ended ODU UNI, on page 491.	For ODU UNI circuit type when the Bandwidth field is set to ODU0, ODU1, ODU2, or ODU2E.
Z-End Open Ended	Check this check box to create an open-ended circuit, in which the destination end point is connected to an ODU subcontroller, instead of a client payload controller. **Note** Checking this checkbox will not deploy ODU subcontrollers on the Cisco NCS 4000 devices. You must configure the ODU subcontrollers on the Cisco NCS 4000 devices before adding the devices to Cisco EPN Manager. For more information about the open ended ODU UNIs and how to configure ODU subcontrollers on Cisco NCS 4000 devices, see Open Ended ODU UNI, on page 491.	For ODU UNI circuit type when the Bandwidth field is set to ODU0, ODU1, ODU2, or ODU2E.
Service Type	Service types supported for the selected bandwidth. See Table 42: Value Mapping—Bandwidth and Service Type for ODU UNI Circuits for the mapping of values in the Bandwidth and Service Type fields.	For ODU UNI circuit type.

Attribute	Description	Enabled
Route Properties		
Bit Rate	Total number of bits per second.	For all OTN circuit types (except ODU UNI Hairpin) when the Bandwidth field is set to ODUFLEX.
Framing Type	The elementary signal of the requested service. Values are: • CBR—Constant bit rate. • GFP-F-Fixed—Fixed and frame mapped generic framing procedure.	For all OTN circuit types (except ODU UNI Hairpin) when the Bandwidth field is set to ODUFLEX.
Record Route	Check this check box to record the circuit route.	For all OTN circuit types (except ODU UNI Hairpin).

Endpoint Section Reference for OTN Circuit Types

The following table lists and describes the attributes that define the protection type and path options for OTN circuit types.

Table 41: Endpoint Section Reference—OTN Circuit Types

Attribute	Description	Enabled
Endpoints		
Device Name	A end and Z end devices of the circuit. **Note** For ODU UNI Hairpin circuits, both A end and Z end will be the same device but with different termination points.	For all OTN circuit types.
Interface	Interface names for the A end and Z end devices.	For ODU UNI circuits.
Termination Point	Termination point for the cards.	For OPU over ODU and ODU UNI Hairpin circuits.

Attribute	Description	Enabled
Protection Type	Protection type for the OTN circuit. Values are: • 1+0—Unprotected card. If a failure is detected in the working path, it results in loss of data. • 1+1—Both primary and secondary path carry traffic end to end and the receiver receives and compares both the traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path. • 1+R—When the primary path fails, the restored path is calculated and traffic is switched to the restored path. If the primary path is non-revertible, the restored path becomes the new primary path. • 1+1+R—Both primary and secondary path carry traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path. The restored path is calculated and traffic is switched to the restored path. If the primary or secondary path is non-revertible, the restored path becomes the new primary or secondary path. **Note** This protection type is not supported for Cisco NCS 4000 series devices.	For all OTN circuit types (except ODU UNI Hairpin).
Diverse From Tunnel ID	Select a tunnel to ensure that it is not used by the circuit you are provisioning. This is to ensure that if there is a failure in a tunnel, the same tunnel is not used by another circuit.	For all OTN circuit types(except ODU UNI Hairpin).
Working Path,**Protected Path**, and **Restored Path** The Protected Path field group is available for all OTN circuit types (except ODU UNI Hairpin) only when the Protection Type field is set to 1+1 or 1+1+R. The Restored Path field group is available for all OTN circuit types (except ODU UNI Hairpin) only when the Protection Type field is set to 1+R or 1+1+R.		
Type	Choose the type of working path or protected path for the circuit. Values are Dynamic and Explicit.	For all OTN circuit types (except ODU UNI Hairpin).
New	Check this check box to create a new explicit working or protected path for the circuit.	For all OTN circuit types (except ODU UNI Hairpin) when the Type field is set to Explicit.

Attribute	Description	Enabled
Select Existing EP	Choose an existing explicit working or protected path for the circuit.	For all OTN circuit types (except ODU UNI Hairpin) when the Type field is set to Explicit and the New check box is unchecked.
New Name	Enter a name for the explicit path that you are creating. In the table below the New Name field, click the '+' button to add a new row to the table, and then select a device and an explicit path controller as the interface for the device.	For all OTN circuit types (except ODU UNI Hairpin) when the Type field is set to Explicit and the New check box is checked.
Protection Profile The Protection Profile field group is available for all OTN circuit types (except ODU UNI Hairpin) only when the Protection Type field is set to 1+1, 1+R, or 1+1+R and a valid A end device is selected.		
Protection Profile	The profile used to manage the protection of the circuit. This protection profile must be configured on the A end node of the circuit. **Note** You can enter the protection profile that was configured on the device. The details of the protection profile such as the protection type, SNC, hold off, wait to restore, and whether the circuit is revertive are displayed.	

Bandwidth and Service Type Value Mapping for ODU UNI Circuits.

The following table maps the values in the Bandwidth and Service Type fields for the ODU UNI circuits

Table 42: Value Mapping—Bandwidth and Service Type for ODU UNI Circuits

Bandwidth	Service Type
ODU0	• Ethernet OPU0 GMP
ODU1	• OTN OPU1 • Sonet OPU1 BMP • SDH OPU1 BMP
ODU1E	• Ethernet OPU1e BMP • OTN OPU1e

Bandwidth	Service Type
ODU1F	• OTN OPU1f
ODU2	• Ethernet OPU2 GFP_F • Ethernet OPU2 GFP_F_EXT • Ethernet OPU2 WIS • OTN OPU2 • Sonet OPU2 AMP • Sonet OPU2 BMP • SDH OPU2 AMP • SDH OPU2 BMP
ODU2E	• Ethernet OPU2e BMP • OTN OPU2e
ODU2F	• OTN OPU2f
ODU4	• OTN OPU4 • Ethernet OPU4 GFP_F • Ethernet OPU4 GMP
ODUFLEX	• OTN OPUFlex • Ethernet OPUFlex GFP_F

Create and Provision an ODU Circuit

To create and provision an ODU circuit:

Before you begin

- For information about the prerequisites that must be met before provisioning an optical circuit, see Prerequisites for Provisioning Optical Circuits, on page 528.
- To create managed links among devices, see Manually Add Links to the Topology Map, on page 180.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and select the location where you want to create the ODU circuit.

Step 3 Close the **Device Groups** pop-up window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar. The Provisioning Wizard opens in a new pane.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Optical**. Cisco EPN Manager displays a list of relevant circuit types in the Service Type area.

Step 7 In the **Service Type** area, choose **ODU**.

Step 8 If you have defined profiles to set the attributes of different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the **Customer Section** page.

Step 10 (Optional) Select the customer for the circuit. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and restart the Provisioning Wizard.

Step 11 Enter the circuit name and description in the **Customer Section** page.

Step 12 Click **Next** to go to the **Circuit Section** page.

Step 13 You can create two types of ODU circuits here: **Remote** ODU circuit and **Local** ODU circuit.

To create a **Remote** ODU circuit (ODU circuit between two different devices):

a) Uncheck the **Local Cross Connect** check box.

Choose one of the following protection type for the circuit:

None—No protection type for the circuit.

1+1—Both primary and secondary paths carry the traffic end to an end. The receiver receives the traffic from primary and secondary paths, and compares both the traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path.

Note If you have selected 1+1 as the protection type, the Connection Mode is set to SNC-N, by default.

To create a **Local** ODU circuit (cross-connection within the same device):

Step 14 Choose the required Reversion Time and Hold off Timer for the circuit.

Note These fields are available only if you have selected 1+1 as the protection type.

Step 15 Click **Next** to go to the **Endpoint Section** page.

Step 16 Select a row in the Endpoint table, and then click a device in the map to populate the Device Name column with the selected device. Alternatively, you can click the row in the Endpoint table to edit the Device Name and Termination Point columns. Only network elements that are available and compatible with the chosen circuit type will be displayed.

Note When the row is in the edit mode, you cannot click a device in the map to populate the **Device Name** column.

Step 17 Click **Next** to go to the **Constraints Section** page.

Step 18 Click a device node in the map to add it to the Constraints table. Alternatively, you can click the '+' button in the table toolbar to add a new row to the table and edit the Node/Link Name, Include/Exclude, and Route columns. Only network elements that are compatible with the ODU circuit type will be displayed.

Note You cannot provide links as constraints for ODU circuits.

Step 19 (Optional) Click **Calculate Path** to verify if there is a valid working path between the selected endpoints. If a valid working path exists between the selected endpoints, the path appears with a 'W' label on the topology map. If a valid working path does not exist between the selected endpoints, a Path Calculation Result section appears that displays the reason why a working path cannot be established between the selected endpoints.

Step 20 Click **Create Now** to create the circuit. If you want to see a preview of the TL1 or CLI commands that will be deployed to the devices, click **Preview**. You can either deploy the configurations to the device or cancel it, but you cannot edit the attributes.

Step 21 To create a **Local** ODU circuit (cross-connection within the same device):

a) Check the **Local Cross Connect** check box.

b) Select the circuit properties such as **Bandwidth** and **Service type**.
c) Choose one of the following protection type for the circuit:

None—No protection type for the circuit.

1+1—Both primary and secondary paths carry the traffic end to an end. The receiver receives the traffic from primary and secondary paths, and compares both the traffic. When the egress node detects failure in one path, it switches the traffic to the unaffected path.

Note If you have selected 1+1 as the protection type, the Connection Mode is set to SNC-N, by default.

d) Choose the required Reversion Time and Hold off Timer for the circuit.

Note These fields are available only if you have selected 1+1 as the protection type.

e) Click **Next** to go to the **Endpoint Section** page.
f) Select the **Device Name**, inside which you want to provision an ODU circuit.
g) Select the **Source**, **Secondary Source/Destination**, and **Destination** ports. Select the **ODU** slices.

Note **Secondary Source/Destination** is only available if you have selected 1+1 as the protection type.

h) Click **Create Now** to create the circuit. If you choose to see a preview of the circuit, click **Preview**. You can either deploy the configuration to the device or cancel it, but you cannot edit the attributes.

The circuit will be added to the list in the Circuits/VCs pane in the Network Topology window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Discovery and Provisioning of ODU Circuits Between Cisco NCS 2000 Series and Cisco NCS 4000 Series Devices

Cisco EPN Manager supports provisioning of end-to-end ODU circuits between Cisco NCS 2000 series and Cisco NCS 4000 series devices.

ODU circuit provisioning between Cisco NCS 2000 series and Cisco NCS 4000 series devices involves discovery of OTU links between their end nodes, after which the circuit can be provisioned.

To discover OTU links between Cisco NCS 2000 series and Cisco NCS 4000 series devices, see Discovering OTU Links Between Cisco NCS 2000 Series Devices and Cisco NCS 4000 Series Devices, on page 552.

To create an ODU circuit between any endpoints, see Create and Provision an ODU Circuit.

Prerequisites to provision ODU circuits:

- To provision end-to-end circuits, the client ports must have free endpoints.

Cisco EPN Manager supports the following scenarios for discovering and provisioning ODU circuits between Cisco NCS 2000 series and Cisco NCS 4000 series devices:

- **Brownfield discovery with ODU UNI circuits (between Cisco NCS 4000 series devices) and local ODU XC circuits (between Cisco NCS 2000 series devices).**

  In this scenario, an ODU circuit is provisioned between Cisco NCS 2000 series devices with Cisco NCS 4000 series devices as the mid-nodes. To provision this ODU circuit:

  1. Create local ODU cross-connects on the nodes of participating Cisco NCS 2000 series devices.

2. Create ODU UNI circuits on the nodes of participating Cisco NCS 4000 series devices.
3. Use the OCH-Trials (discovered on OCH-NC WSON circuits) to connect the nodes of Cisco NCS 2000 series and Cisco NCS 4000 series devices. On successful OCH-Trial connection between these nodes, an OTU link will be discovered.
4. An ODU circuit will be discovered on top of the above-mentioned circuits with the circuit name: *E2E:<local odu xc name Aend>---<local odu xc name Zend>*.

Note Promote/Modify/Delete operations are not supported on Brownfield ODU circuits.

Note Brownfield discovery is not supported when static cross-connects exist on the Cisco NCS 4000 series devices.

Note ODU UNI circuits must not be created on the ports of Cisco NCS 4000 series devices that form a part of the ODU circuit.

- **Greenfield discovery between Cisco NCS 2000 series and Cisco NCS 4000 series devices.**

  In this scenario, ODU circuits are provisioned between Cisco NCS 2000 series devices, or between Cisco NCS 2000 series devices and Cisco NCS 4000 series devices.

  In this case:

  - OTU links are discovered on top of an OCH-Trail WSON (Cisco NCS 2000 series devices to Cisco NCS 2000 series devices), or on top of an OCH-Trail (Cisco NCS 2000 series devices to Cisco NCS 4000 series devices). Create an ODU circuit on top of these discovered OTU links.
  - You can choose OTU links as constraints.

Discovering OTU Links Between Cisco NCS 2000 Series Devices and Cisco NCS 4000 Series Devices

To provision a successful end-to-end ODU circuit between the Cisco NCS 2000 series and Cisco NCS 4000 series devices, an OTU link must be discovered.

To successfully discover an OTU link:

1. Create GMPLS LMP circuits between the participating Cisco NCS 2000 series and Cisco NCS 4000 series devices (Trunk and ADD/DROP ports). OCH links appear in the topology between the trunk and ADD/DROP ports.
2. Create OCH-NC WSON circuits between the participating Cisco NCS 2000 series devices (ADD/DROP ports).

3. On successful creation of OCH-NC WSON circuits, an OCH-Trail is discovered between the devices, which prompts the discovery of an OTU link between the trail endpoints.

Note To successfully discover an OTU link, the OCH-Trail must be in the FULL state.

Note If an OCH-Trail is discovered on the ports of an existing OTU link (created using the managed link), then the existing OTU link (Managed) is converted into the discovered OTU link.

Provision L3VPN Services

Features and Limitations of L3VPN Provisioning

To know more about supported L3VPN services, see Supported L3VPN Services, on page 494.

Cisco EPN Manager supports the following L3VPN features:

- Creation of VRFs
- Automatic allocation of Route Target IDs
- Automatic allocation of route distinguishers
- Discovery of VPNs consisting of several VRFs, based on multiple criteria (VPN ID, common name, and provisioning naming conventions)

  You can select devices for L3VPN provisioning using the Point and Click method of provisioning.
- Definition of IP endpoints attached to a VRF
- Associating ethernet subinterfaces with VRFs
- Provisioning of BGP and/or OSPF neighbors between CE and PE
- Attaching QoS profiles to the endpoint interfaces

- Adding new VRFs to existing VPNs
- Modifying VPNs and associated VRFs created and deployed (or discovered and promoted)
- Overlays in the Network Topology for L3VPN services
- Promotion of L3VPN services discovered directly from the device
- Using route targets with OSPF dual AS routing
- Using integrated routing and bridging to provision L3VPN services using BDI/BVI interfaces (subinterfaces)
- Associating IP Service Level Agreements (SLAs) and CLI templates with L3VPN services
- Route redistribution between the PE-CE link and the MP-BGP core using connected, static, RIP, or OSPF routes
- Provisioning L3VPN services using LAG interfaces
- Provisioning L3VPN services using HSRP
- Mapping of L2 circuits to L3VPN services

  You can see these L2VPNs under the **Circuit/VCs 360 view** > **Related Circuits/VCs** tab.

  To show or hide the L2 circuits associated with the L3VPN service in the **Network Topology** overlay, navigate to **Administration** > **Settings** > **System Settings** > **Discovery Settings** > **L3L2 Circuit Mapping** tab, and enable/disable the checkbox **Enable L3L2 Mapping**.

Cisco EPN Manager has the following L3VPN limitations:

- For the list of devices that support VRFs, see Cisco Evolved Programmable Network Manager Supported Devices.
- You cannot provision multicast VPNs, only unicast VPNs are supported.
- While creating the L3VPN service, you may add any number of VRFs to the VPN. However, it is not recommended to add more than 5 VRFs. You can add more VRFs later to the VPN using the **Modify VRF** and **Add VRF** options. An L3VPN service can contain a maximum of 15 endpoints, if it is provisioned through a green field.
- Only one VRF per device is supported. You can create multiple VRFs but on different devices (with the same VRF name or different VRF names).
- Route policies can be selected but cannot be defined within the L3VPN service.
- Only BGP, OSPF, and OSPFv3 routing protocols are supported in PE-CE.
- There is no support for multiple attached PEs, so there is no Site of Origin support.
- Deleting an L3VPN service deletes the IP SLA operations associated with the service from the device. The associated operations that are deleted will not be available for future usage.
- The Integrated Routing and Bridging (IRB) is not supported for Cisco Catalyst 6500 series switches.
- Modification of Route Distinguisher through Modify VRF flow is supported only for IOS XR devices.

- Maximum of 15 endpoints are supported in Modification/Deletion of a fully discovered L3VPN service post promotion. To configure the **Maximum Number of Endpoints** for L3VPN promotion, navigate to **Administration** > **Settings** > **System Settings** and select **Discovery Settings** in the **Circuits/VCs**.
- Maximum of 50 endpoints are supported while mapping L2 circuits to L3VPNs. To configure the **Number of L3L2 Endpoints**, navigate to **Administration** > **Settings** > **System Settings** > **Discovery Settings** > **L3L2 Circuit Mapping** tab.

Prerequisites for L3VPN Provisioning

Before you begin provisioning L3VPN services, ensure that the following prerequisites are followed.

Following are the prerequisites for provisioning an L3VPN service:

- BGP must be set up on all devices. Typically all devices must communicate with each other via a pair of route reflectors.
- Preconfiguration changes required to set up BGP:

  Configure the BGP router-id as shown in the example below:

  ```
  router bgp 65300
      bgp router-id 10.1.1.1
  ```

  Set Vpn4 and Vpn6 as the parent address family using these commands:

  ```
  router bgp 100
  address-family vpnv4 unicast
  address-family vpnv6 unicast
  ```

- MPLS reachability must be set up between the devices. MPLS core network configuration must be set up.
- Inventory collection status for the devices on which the L3VPN services will be provisioned must be 'Completed'. To check the status of devices, go to **Inventory > Network Devices**, and look at the status in the **Last Inventory Collection Status** column.
- Before you provision a L3VPN service with IPv6 address family on XE devices, IPv6 routing must be enabled. To enable IPv6 routing, configure the command:

  ```
  ipv6 unicast-routing
  ```

- (Optional) Customers must be created in the system so that you can associate the L3VPN service to a customer during L3VPN service provisioning. To create and manage customers, choose **Inventory > Other > Customers**.

L3VPN Service Discovery

The Cisco EPN Manager supports the discovery of large L3VPN circuits with upto 40,000 endpoints and 4000 VRFs.

The Cisco EPN Manager associates multiple VRFs into a single VPN using multiple criteria:

- If VRFs were configured with a VPN ID, then the VPN service is discovered using the VPN ID to identify the VRFs that belong to the same VPN. If you have VPNs that you need to discover, where different VRF names are used within one VPN, then the Cisco EPN Manager discovers VRFs by the VRF names.

  If one VRF is created per device, it is common practice to simply use the same VRF name everywhere across the VPN. If the Cisco EPN Manager sees multiple VRFs with the same name and no VPN ID, then it considers them as a single VPN, and the VPN name will be the name of the VRFs.

- VRFs with the same names and numbers will belong to the same VPN. For example, these are VRFs belonging to a VPN called 'ABC':

  V1:ABC, V2:ABC, V4:ABC-s, V22:ABC-h, V001:ABC, and so on.

- If VRF has no VPN ID and has a unique name that doesn't match other names according to the provisioning convention, it will be placed as an individual VPN. The name of the VPN will be the name of the VRF.

The provisioning naming convention feature is driven by a regular expression that is embedded in the product. If configuring a VPN is not an option for you and you have a naming convention that can be matched with a regular expression, it is possible to change it. To change the regular expression, please contact your Cisco Advanced Services representative.

Create and Provision a New L3VPN Service

The process of creating and provisioning a unicast L3VPN involves:

- (Optional) Associating a customer to the VPN.
- Defining the attributes that influence how traffic that is delivered over the L3VPN and through its endpoints will be treated.
- Specifying the endpoints and route redistribution values of the L3VPN.
- (Optional) Configuring IP Service Level Agreements (SLAs) operation to monitor end-to-end response time between devices using IPv4 or IPv6.
- (Optional) Associating user-defined CLI templates with the L3VPN service.

Note: Only Unicast L3VPN services are supported in this release.

To create a new L3VPN service:

Step 1 From the left pane, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2 From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.

Step 3 Click the **Circuits/VCs** tab, then click the **+** (**Create**) icon in the **Circuits/VCs** pane toolbar.

The Provisioning Wizard opens in a new pane to the right of the map. You can also access the L3VPN Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.

Step 4 From the **Technology** drop-down list, select **L3VPN**. A list of supported L3VPN service types is displayed.

Step 5 In the **Service Type** section, choose **Unicast** and click **Next** to enter the customer and service details. In this release, the only supported service type is Unicast L3VPN.

Step 6 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list.

Step 7 (Optional) Select the customer that you want to associate with the VPN. If there are no customers in the drop-down list, you can go to **Inventory > Other > Customers** to create the customer and return to this step.

Step 8 Specify the basic L3VPN parameters:

a) Use the **Activate** check box to specify whether the service must be in active (check box enabled) or inactive (check box disabled) state. The Active state enables traffic to pass through the circuit and automatically sets the Service State for all associated IP endpoints to True. In the Inactive state, you can choose to set the service state for IP endpoints to true or false.

b) Provide a unique name for the service and optionally enter a description.

c) Enter a unique VPN ID for the service. The VPN ID must be in the format OUI:VPN Index. For example, 36B:3. Here, 36B is the Organization Unique Identifier (OUI) and 3 is the VPN Index.

d) In the **IP MTU** field, enter a value between 1500 (default) and 9216. The service MTU is the size in bytes of the largest IP packet that can be carried unfragmented across the L3VPN. It does not include layer 2 headers.

The configured interface MTU is the service MTU plus the size of any layer 2 headers. For Ethernet, this adds 14 plus 4 bytes per VLAN header.

The value of the UNI MTU depends on the service MTU and outer and inner VLAN values:

- If both outer and inner VLANs are present, then the UNI MTU value is greater than the Service MTU + 14 + (4*2)
- If only the outer VLAN is present, then the UNI MTU value is greater than the Service MTU + 14 + (4 *1)
- If no VLANs are present, then the UNI MTU value is greater than the Service MTU + 14.

e) (Optional) To create a full mesh topology for this service, select the **Create Full Mesh** check box and enter the full mesh prefix manually in the **New Prefix** field or select a value from the **Existing Prefix** drop-down list. The available options depend on the full mesh prefix values that are discovered in the selected device.

f) Select the address family as **IPv4, IPv6,** or **Both** in the **Full Mesh Address Family** drop-down list.

Step 9 Use the **Route Target Allocation** section to manually specify the route target address families (**IPv4, IPv6, or Both**) and their associated route target values. You can create multiple route targets for the L3VPN service. These route targets can be associated with any VRF that you attach to this L3VPN service in the following steps.

Note The route targets associated with a VRF must also be associated with the L3VPN the VRFs belong to.

Note The configured route policy is listed in the **Export** drop-down list of the route policy.

Step 10 In the **Deployment Action** drop-down list, specify the task that must be taken up when the service creation process is completed. Your options are:

- **Preview**: allows you to review the configuration that is generated before it is deployed to the device.
- **Deploy**: allows you to deploy the configuration to the relevant devices immediately upon completion.

Step 11 Click **Next** to associate VRFs to the L3VPN service.

Step 12 Select the required VRFs from the **VRFs** drop-down list or add a new VRF as explained below, and then click **Next**. During L3VPN service creation, you can associate up to five VRFs with the VPN. To associate more VRFs to the VPN, see Add and Copy VRFs to an L3VPN Service, on page 572. To create a new VRF:

a. Click the '+' icon to add the VRF details manually. To auto populate the VRF details, click the respective device on the map. The device details and a new name for the VRF are automatically populated on the Add VRFs page.

b. To manually specify the VRF details, select the required device in the **Device** drop-down list. You can then manually enter the VRF name and description, and check the **RD Auto** check box.

Note If multiple VRFs are created on the same device, you must name them differently to ensure that they are not part of the same VPN. You cannot create multiple VRFs with the same names on the same device.

Step 13 Specify the IPv4 and IPv6 route targets and route distribution details:

a. Route Targets: Select the route targets for this VRF in the **Route Target** drop-down list. The options in this drop-down list are available based on the route targets associated with this service in Step 7.

b. Select the direction in which the route targets must be applied. Depending on the device you select, choose **Import**, **Export**, **Both**, or **None**.

Choose the directions depending on the type of device that is selected. For example, for Cisco IOS-XR devices, you cannot choose 'None' as the route target direction.

c. In the **Route Policy** section, select the import and export policy for the route targets.

Note **Route Policy** which has Opaque Extended Community that is attached is applicable only for export.

d. In the **Route Distribution** section, specify the protocol that must be associated with the VRF, the protocol's metric value, the routing process ID, the relevant route policies and the route match type.

- **Protocol**- Choose the source protocol from which routes must be redistributed. Your options are Static, Connected, RIP, and OSPF.
- **Metric**- (Optional) Enter a numeric value for the metric which is used when redistributing from one routing process to another process on the same router.
- **Routing Process ID**- (applicable only to OSPF and RIP) Specify the unique numerical value that identifies the instance of the routing process on the device.
- **Route Policy**- (Optional) Select one of the route policies present on the selected device. You cannot create route policies using Cisco EPN Manager.

  Note **Route Policy** which has Opaque Extended Community that is attached cannot be used in Redistribute.

- **Route Match Type** (applicable only to OSPF)- Select the appropriate match type in the drop-down list associated with the selected route policy.

Step 14 Specify the IP endpoints and UNIs' values manually as follows:

- If the endpoint interface has already been configured as a UNI, uncheck the **New UNI** check box and select the required UNI from the **UNI Name** drop-down list.
- To create a new UNI:
  a. Select the **New UNI** check box.
  b. In the **UNI Name** field, enter a unique name for the UNI.
  c. In the **Device** drop-down, select the device, its required interface, and provide a description for the UNI.

d. Check the **Service Multiplexing** check box to enable more than one L3VPN or Carrier Ethernet service to be supported at the UNI.

e. Specify the IP Maximum Transmission Unit (MTU) for the UNI., the speed and duplex settings for the UNI.

f. Either check the **Auto Negotiation** check box to automatically adjust the speed and duplex settings for the UNI or uncheck the **Auto Negotiation** check box and specify the speed and duplex settings manually.

g. Choose the UNI QoS profiles for ingress or egress traffic on the UNI. The list of profiles includes policy maps that were configured on the device and discovered by the system, and user-defined QoS profiles. If you select a UNI QoS profile, you cannot add individual QoS policies to the service endpoint in the upcoming steps. If you want to add specific QoS policies to the endpoint, leave the UNI Ingress and Egress QoS Profile fields blank.

Note You can choose two different discovered QoS profiles for the ingress and egress directions, however, in case of user-defined QoS profiles, only a single QoS profile can be chosen for both directions.

h. Select **Enable Link OAM** to enable IEEE 803.1ah link operation and maintenance. If Link OAM is enabled, you will see events relating to the state of the link between this UNI and the customer's access switch.

i. Select **Enable Link Management** to enable the customer access switch to get information about this UNI, VLAN IDs, services on the UNI, and so on.

For a detailed description of the fields and attributes in the UNI table, see New UNI Details Reference, on page 516.

Step 15 Specify the service endpoint to be associated with the L3VPN by providing the following details, and then click **Next**:

- **VRF Name**: Choose one of the available VRFs that can be associated with this VPN.
- **IPv4 and IPv6 address**: Enter the IP addresses and network masks of the service endpoint. The masks can be entered simply as an integer that represents the length of the network mast (or in CIDR format).
- **VLAN and Inner VLAN**: Enter the inner and outer VLAN identifiers using integers between 1 and 4094. Inner VLAN is the identifier for the second level of VLAN tagging.
- **QoS Policy**: (Optional) Select the QoS policy that must be applied to the service endpoint. This field is disabled if you have associated UNI Ingress/Egress QoS profiles to the service in the above step. For information on creating QoS profiles, see Configure Quality of Service (QoS) , on page 436.

  Note You can choose two different discovered QoS policies for the ingress and egress directions, however, in case of user-defined QoS policies, only a single QoS policy can be chosen for both directions.

- **Service State**: Specify whether the service state for associated IP endpoints must be set to true or false. If the L3VPN is in Activate state (specified in Step 6 above), this check box is disabled and all service state values are automatically set to True.
- **Use Integrated Routing & Bridging**: Specify whether the VRF and IP addresses must be configured under the subinterfaces or under the BVI (virtual) interfaces.

  Note This check box is enabled only when you select devices such as Cisco ASR 90XX devices, which support integrated routing and bridging. For Cisco ASR90x and other IOS-XE devices you cannot uncheck the **Use Integrated Routing & Bridging** check box because configuration is taken care by the BDI interface..

- (Optional) Check the **Enable HSRP** check box to specify the HSRP details. See HSRP Details Reference, on page 563

Step 16 Click **Next** to go to the **PE-CE Routing** page.

Step 17 Click the '+' icon to add the PE-CE routing details. See PE-CE Routing Details References, on page 564.

Step 18 (Optional) Select existing IP SLA parameters from the list, or specify the IP SLA operation parameters that are described in the table below and then click **Next**.

IP SLA Settings	IP SLA Parameters	Descriptions
Operation Settings	Name	Enter a unique name to identify the IP SLA operation for the selected L3VPN service.
	Type	Select the type of IP SLA operation that must be generated for the devices participating in this L3VPN service. Your options are: • **UDP Echo**: Configures an IP SLAs User Datagram Protocol (UDP) Echo operation to measure response times and to test end-to-end connectivity between a Cisco device and devices using IPv4 or IPv6. • **ICMP Echo**: Allows you to measure end-to-end network response time between a Cisco device and other devices (source and destination values, as described below) using IPv4 or IPv6. With an IP SLA operation of type ICPM Echo, you cannot associate the 'Connection Loss' action variable. • **UDP Jitter**: Configures the UDP jitter operation which analyzes round-trip delay, one-way delay, one-way jitter, one-way packet loss, and connectivity in networks that carry UDP traffic in IPv4 or IPv6 networks.
	Source	Specify the device which acts as the source point from which the IP SLA configuration is generated. The IP SLA responses are generated based on the connectivity between this source device and the target device. The VRF values for this operation are automatically selected based on your Source selection.
	Source Port	Enter a numeric value between 0 and 65535 to specify the source port value for which the IP SLA operation must be configured.
	Destination	Specify the device which acts as the target point from which the IP SLA configuration is generated. The IP SLA responses are generated based on the connectivity between the source device and this target device.
	Destination Port	Enter a numeric value between 0 and 65535 to specify the destination port value for which the IP SLA operation must be generated.
	VRF	The VRF details are automatically selected based on the device that you specify as the IP SLA operation Source.

IP SLA Settings	IP SLA Parameters	Descriptions
Reaction Settings	Action Variable	Select the variable based on which the IP SLA reactions must be triggered. For example, when a monitored value exceeds or falls below a specified level, or when a monitored event (such as a timeout or connection loss) occurs. • **Connection Loss**: Indicates that an event must be triggered when a connection loss occurs. This value is not displayed if you select ICPM Echo as the type of operation. • **Round Trip Time**: If you choose this action variable, you must enter the **Upper Threshold Value** and the **Lower Threshold Value** which indicates that an event must be triggered when a monitored value exceeds or falls below the upper and lower threshold values that you specify. • **Time Out**: Indicates that an event must be triggered after a given set of consecutive timeouts occur. • **Verify Error**: Indicates that an event must be triggered after an error of type 'VerifyError' occurs.
	Action Type	Select one of the following actions that must be taken based on the conditions set in the Action Variable field: • **None**: No action is taken. • **Trap and Trigger**: Triggers both an SNMP trap and starts another IP SLAs operation when the violation conditions are met, as defined in the Trap Only and Trigger Only options below. • **Trap Only**: Sends an SNMP logging trap when the specified violation type occurs for the monitored element. • **Trigger Only**: Changes the state of one or more target operation's Operational state from 'pending' to 'active' when the violation conditions are met. A target operation continues until its life expires (as specified by the target operation's configured lifetime value). A triggered target operation must finish its life before it can be triggered again.
	Threshold Type	

IP SLA Settings	IP SLA Parameters	Descriptions
		Select the threshold type based on which the IP SLA events are generated. • **Average**: If you choose this threshold type, enter the **N Value** which specifies that an event must be triggered when the averaged total value of N probes is reached either when specified upper-threshold value is exceeded, or when it falls below the lower-threshold value. • **Consecutive**: If you choose this threshold type, enter the **Consecutive Values** as part of the reaction settings. This threshold type triggers an event only after a violation occurs a specified number of times consecutively. For example, if you enter 5 as the consecutive value, the consecutive violation type is used to configure an action to occur after a timeout occurs 5 times in a row, or when the round-trip-time exceeds the upper threshold value 5 times in a row. • **Immediate**: Triggers an event immediately when the value for a reaction type (such as response time) exceeds the upper threshold value or falls below the lower threshold value, or when a timeout, connection loss, or verify that error event occurs. • **Never**: Never triggers an event. • **X out of Y occurrences**: If you choose this threshold type, enter the **X Values** and **Y Values** to specify the number of occurrences. This triggers an event after some number (x) of violations within some other number (y) of probe operations (x of y).
Simple Schedule	-	Enter the scheduling parameters for an individual IP SLAs operation by entering the following values: • **Frequency**: Enter the elapsed time within which the operation must repeat, in seconds. • **Life Time**: Enter the overall time until when the operation must be active, in seconds. A single operation repeats at the specified frequency for the lifetime of the operation. • **Age Out**: Enter the length of time to keep an operation active, in seconds. For example, an age out value of 43200 will ensure that the operation will age out after 12 hours of inactivity. • **Start Now** and **Start After**: Enable the Start Now check box to schedule the IP SLA operation to be executed immediately on Save. Or use the Start After field to specify the number of minutes after which the operation can be executed.

Step 19 (Optional) Use the Service Template page to append a template with additional CLI commands that will be configured on the devices participating in the service. See Extend a Circuit/VC Using Templates, on page 609 for more information.

Step 20 When you have provided all the required information for the service, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the L3VPN attributes. Otherwise, the configurations will be deployed to the devices immediately.

In case of a deploy failure on even a single device that is part of the service, the configuration is rolled back on all devices participating in the service. To delete the endpoints associated with the service, see, Delete an L3VPN Service Endpoint, on page 654. To add more VRFs to this L3VPN service, see Add and Copy VRFs to an L3VPN Service, on page 572.

HSRP Details Reference

Hot Standby Router Protocol (HSRP) is Cisco's standard method of providing high network availability by providing first-hop redundancy for IP hosts on an IEEE 802 LAN configured with a default gateway IP address. Hot Standby Router Protocol (HSRP) provides redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop router failures. HSRP allows multiple routers on a single LAN to share a virtual IP and MAC address which is configured as the default gateway on the hosts. In the group of routers configured in an HSRP group, there is one router that is elected as the active router and another as a standby router. The active router assumes the role of forwarding packets that are sent to the virtual IP address. If the active router fails, the standby router takes over as the new active router. In Cisco EPN Manager, HSRP for IPv4 is supported on switches running the IP base or IP Services image and HSRP for IPv6 is supported on unicast routing. HSRP is not supported in IOS-XE devices for address family IPv6. The following table lists and describes the attributes of HSRP.

Table 43: HSRP Settings

Attribute	Description
Group Number	Enter the standby group number of either IOS-XE or IOS-XR device. The recommended range values are: • Range value for IOS-XE: 0–255. • Range value for IOS-XR: 1–4095.
Virtual IP	Enter the IPv4/IPv6 address. Ensure that the Virtual IP address and SEP address should be entered within the same subnet.
Priority	Enter the priority to decide which router is to be the primary router. Priority range value: 0–255.
Hello Timer	Enter the time between hello packets in seconds. **Note** Hold Timer and Reload Delay values should be entered mandatorily for an IOS-XR device for the specified Hello Timer and Minimum Delay values. Hello time range value: 1–255.
Minimum Delay	Enter the minimum delay time in seconds. Delay range value: 0–10000.
Preempt Minimum Delay	Specify the preempt delay on the router. Delay range value: 0–3600.
Authentication Key	Enter the authentication key if the group number is between 1–255. This allows the authentication messages to be included in the HSRP multicast. This ensures that only authorized routers can become part of the HSRP group.

Attribute	Description
Hold Timer	Enter the hold time in seconds. Hold time range value: 1–255. **Note** Hold down time should be more than hello timer for XE device.
Reload Delay	Enter the delay time to reload. Delay range value: 0–10000.
Preempt Reload Delay	Enter the preempt reload delay. Delay range value: 0–3600. This field is not supported for an IOS-XR device.

PE-CE Routing Details References

The following table lists and describes the attributes that define the PE-CE details for provisioning a Layer 3 VPN service.

Table 44: PE-CE Routing Reference

Attribute	Description
Routing Protocol Settings	
PE Device	Name of the pseudowire device.
VRF	The VRF name that you specified in the VRF page of the wizard is populated.
Routing Protocol Type	Choose,**BGP OSPF**, or **OSPFv3** as the routing protocol for the Layer 3 VPN service. **Note** Based on the routing protocol chosen, either the **BGP Neighbor Information** section or the **OSPF Process Information** section will be displayed. For XR and XE devices the PE-CE authentication is based on the Routing Protocol Type and Authentication Type selection. For more information see, PE-CE Authentication Table.
Address Family	Choose the address family as IPv4 or IPv6. **Note** IPv6 is not supported for the OSPF routing protocol.
Authentication Type	Choose the authentication type. Only the MD5 authentication type is supported. **Note** Authentication Type field is available only when you select OSPF or OSPFv3 as the routing protocol.
BGP Neighbor Information **Note** This section is available only when you select BGP as the routing protocol.	

Attribute	Description
Neighbor Address	Enter the IP address of the neighbor.
Neighbor AS	Enter the autonomous system number of this neighbor, which is the unique identifier used to establish a peering session with a BGP neighbor.
Ingress Route Policy	Enter the route policy applied to any BGP routes received from this neighbor.
Egress Route Policy	Enter the route policy applied to any routes sent to this neighbor.
Local AS	Enter the unique local identifier used to establish a peering session with a BGP neighbor.
AS Action	Select one of the following action types that must be associated with the local autonomous-system (AS) number: • **Prepend**: Use this option to configure BGP such that it prepends the AS number to routes received from the neighbor. • **No Prepend**: Use this option to configure BGP such that it does not prepend the AS number to routes received from the neighbor. • **No Prepend, Replace AS**: Use Replace AS to prepend only the local AS number (as configured with the ip-address) to the AS_PATH attribute. The AS number from the local BGP routing process is not prepended. • **No Prepend, Replace AS, Dual AS**: Use the Dual AS option to configure the eBGP neighbor to establish a peering session. You can do this by using the AS number (from the local BGP routing process) or the AS number configured with the ip-address argument (local-as).
OSPF Process Information **Note** This section is available only when you select OSPF or OSPFv3 as the routing protocol.	
Auto Generate Process ID	By default, this check box is selected to auto generate process IDs. **Note** This check box is only applicable for IOS-XR devices.
Existing Process ID	You can select from the existing process IDs when you uncheck the **Auto Generate Process ID** check box.
Router ID	Specify an IPv4 address for the OSPF protocol.
Area ID	Define an area for the OSPF protocol. The valid range is 0 to 4294967295.
Metric	Specify a numeric value for the OSPF protocol.
Domain Type	Select the required domain type.
Domain Value	Enter the domain value in the 6 Octet Hexadecimal format. For example, 00000000000F.

Attribute	Description
BFD Min Interval	Enter the minimum interval between which control packets are sent to the neighbor. The range is 3–30000 milliseconds.
BFD Min Rx	Enter the minimum Rx value. The range is 3–30000 milliseconds.
BFD Multiplier	The multiplier is the number of times a packet is missed before BFD declares the neighbor down. The range for the OSPF protocol is 2–50 for Cisco IOS-XR and 3–50 for Cisco IOS-XR devices.
BFD Fast Detect	Check this check box to quickly detect failures in the path between adjacent forwarding engines.

Note EPNM allows only one OSPF process to be created for PE-CE routing of a given L3VPN instance. This should be sufficient for XE platforms as single OSPFv3 process can manage both IPv4 and IPv6 address family. But, on IOS-XR platforms, OSPFv3 supports only IPv6 and not IPv4. If customer uses both IPv4 and IPv6 address family,there will be the need for both OSPF and OSPFv3 processes to be created from EPNM.

PE-CE Authentication

The following table lists the relevant combinations of Routing Protocol and authentication types for PE-CE authentication based on the XE and XR devices selection.

Table 45: PE-CE Authentication Reference

Device	Routing Protocol	Authentication Type	Password Type
XE	BGP	—	Click either one of the following radio buttons • Plain Text — Enable to enter the password • Encrypted —Enable to enter an hexadecimal value as the password
	OSPF	—	—
	OSPFv3	Only Key chain authentication type is available. From the Key Chain drop-down list, choose the authentication key chain that is configured on the device.	—

Device	Routing Protocol	Authentication Type	Password Type
XR	BGP	—	Click either one of the following radio buttons • Plain Text — Enable to enter the password • Encrypted —Enable to enter an hexadecimal value as the password
	OSPF	Choose MD5 or Keychain	Click either one of the following radio buttons • Plain Text — Enable to enter the password • Encrypted —Enable to enter an hexadecimal value as the password .
	OSPFv3	Choose either IPSec - MD5 or IPSec-SHA1 as the authentication type.	Click either one of the following radio buttons • Plain Text — Enable to enter the password • Encrypted —Enable to enter an hexadecimal value as the password .

Example Configuration: Provisioning an L3VPN Service

The following are examples of the configuration deployed to a Cisco ASR 9000 device with the following parameters:

- Creation of VRF and IP addresses (both IPv4 and IPv6) under the BDI (virtual) interface.
- Redistribution of OSPF protocol to the BGP protocol.

Example: Provisioning an L3VPN service on a Cisco ASR 9000 device's BVI enabled interface (subinterface).

```
  vrf vrfrbvibdi9k
  vpn id aaaaaa:21
  address-family ipv4 unicast
    import route-target
      6:55
  address-family ipv6 unicast
    import route-target
      6:55
    export route-target
      6:55
interface GigabitEthernet0/0/0/17
  no shutdown
  exit
interface GigabitEthernet0/0/0/17.1
  encapsulation dot1q 1198
  shutdown
interface BVI 1
  vrf   vrfrbvibdi9k
  ipv4 address 88.7.6.4 255.224.0.0
l2vpn
```

```
  bridge group BDI1
    bridge-domain 1
      routed interface BVI 1
      interface GigabitEthernet0/0/0/17.1
router bgp 140
  vrf  vrfrbvibdi9k
    rd auto
    address-family ipv6 unicast
    address-family ipv4 unicast
      exit
    exit
  exit
```

Example: Using a BVI enabled interface for provisioning an L3VPN service with OSPF route distribution (using dual AS):

```
vrf definition VRF2-2VRF-2UNI-BDI
  vpn id AAAAAA:2
  rd 532533:2
  address-family ipv4
    route-target import 6:5
    route-target export 6:5
  address-family ipv6
    route-target export 6:5
interface GigabitEthernet0/0/0
  duplex full
  service instance 2 ethernet
    encapsulation dot1q 761
    bridge-domain 14
    shutdown
  exit
interface BDI14
  vrf forwarding VRF2-2VRF-2UNI-BDI
  ip address 5.44.3.7 255.255.0.0
router bgp 120
  address-family ipv4 vrf VRF2-2VRF-2UNI-BDI
    neighbor 55.4.3.2 remote-as 71
    neighbor 55.4.3.2 activate
    redistribute rip metric 6
    neighbor 55.4.3.2 local-as 387
  address-family ipv6 vrf VRF2-2VRF-2UNI-BDI
    neighbor c5::98 remote-as 50
    neighbor c5::98 activate
    redistribute ospf 65 match external metric 2
    neighbor c5::98 local-as 324 no-prepend replace-as dual-as
    exit
  exit
```

View L3VPN Service Details

Using Cisco EPN Manager, you can view detailed information about an L3VPN service:

- **Circuit/VC 360 View:** The Circuit/VC 360 view provides detailed information available for a specific L3VPN that is created using the Cisco EPN Manager. See View Circuits/VCs. The different parameters associated with the L3VPN service are displayed in five different tabs: Summary, VRFs, Site Details, HSRP, and PE-CE Routing. You can use **Advanced Filters** to search large L3VPN circuits.

Note To view the extended details of HSRP during service discovery, click the **Site Details** tab and choose a row from the IP endpoints. Also, to view the 6VPE authentication properties for the selected OSPFv3 routing protocol type and IPv6 address family, click the **PE-CE Routing** tab.

- **Network Topology and Service Details View:** The Network Topology window presents a graphical, topological map view of devices, links between them, and active alarms on the devices or links. It also enables you to visualize L3VPNs within the displayed topology map.
  - To view a complete list of L3VPNs and its details, see Get Quick Information About a Circuit/VC: Circuit/VC 360 View.
  - To view the L3VPN service details for a specific device, see View a Specific Device's Circuits/VCs
- **Using the Alarms Table:** The Alarms Table in the Cisco EPN Manager displays information about any problems encountered by L3VPN services. See Check Circuits/VCs for Faults.

View HSRP Extended Details

After creating an L3VPN service with Hot Standby Routing Protocol (HSRP) details you can view HSRP properties in the Circuit 360/extended details view.

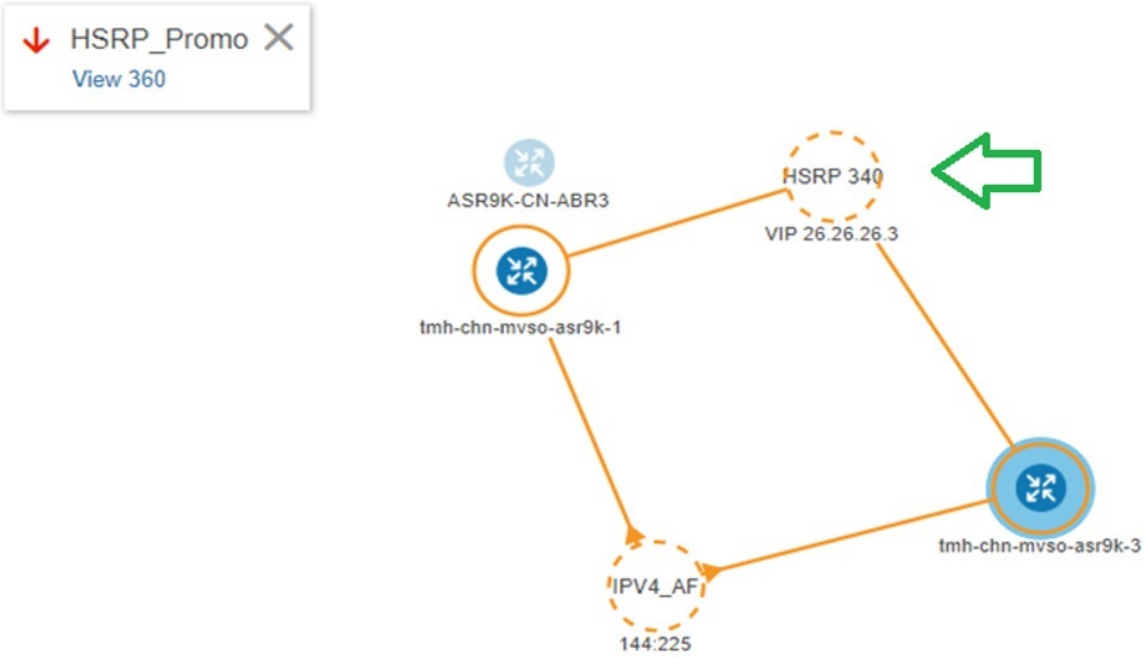
Step 1 From the left pane, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2 From the toolbar, click **Device Groups** and then filter an L3VPN service to view.

Step 3 Choose the L3VPN service to view the Overlay of HSRP as shown in the Figure.

Figure 12: Overlay-HSRP



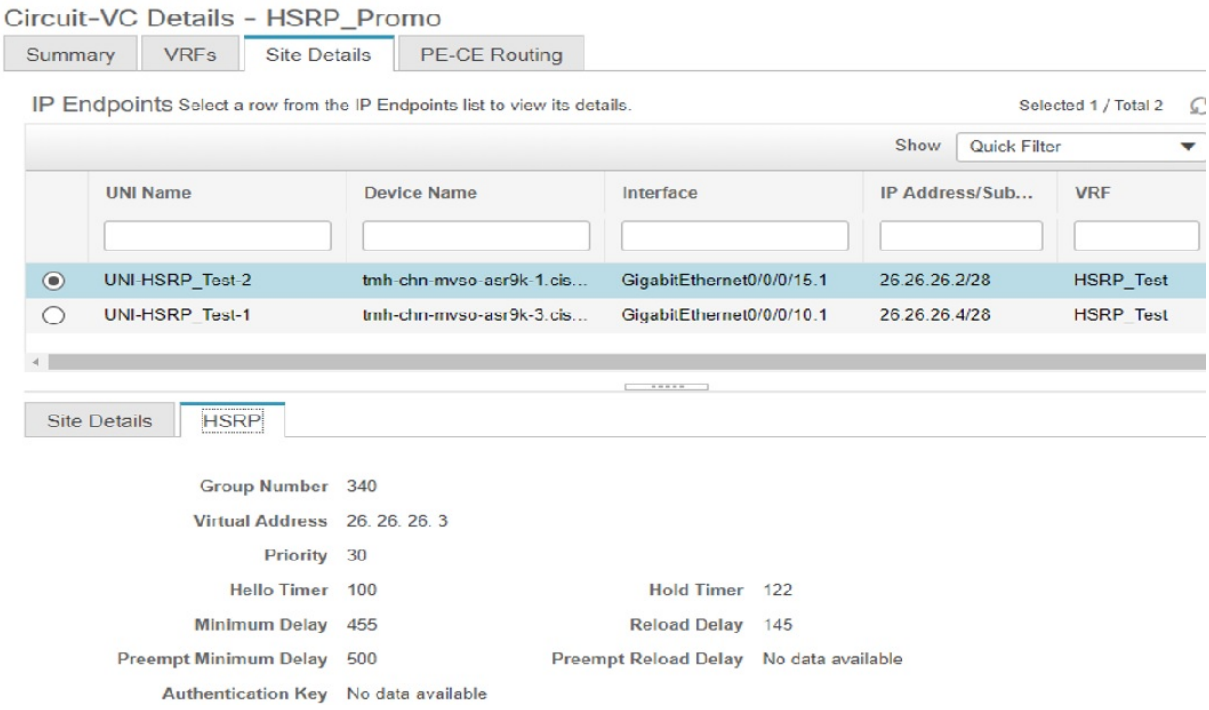
Step 4 Click the HSRP node or the links connected to it to view details relevant to the HSRP as shown:

Figure 13: HSRP Details

Step 5 To view extended details of HSRP:

- Click the View 360 hyperlink. The Circuit/VC 360* page appears.
- Choose **View** > **Details**.
- In the **Circuit-VC Details** window, click the **Site Details** tab.
- Choose an IP Endpoint and then click the **HSRP** tab to view the properties.

Figure 14: Extended Details



Modify L3VPNs and VRFs

You can modify L3VPN services that are created and deployed using Cisco EPN Manager. While the full mesh prefix, QoS profiles, Route Target values, and the OSPF configurations associated with the service can be modified, you cannot modify parameters such as the customer details, VPN name, and service MTU values associated with the service. To modify these parameters, delete the service, and re-create it with new values. You can also modify the VRFs associated with L3VPN services.

To modify L3VPN services and VRFs:

Before you begin

To modify L3VPN services that are discovered and promoted using Cisco EPN Manager, you must ensure that that the route distinguisher for the L3VPN service is specified in the format **rd device_ip:number**. For example:

```
vrf definition vdvvgfr420
  rd 10.104.120.133:420
  vpn id 36B:420
  !
address-family...
```

If the route distinguisher is specified in any other format, you will not be able to edit the service.

Step 1 Navigate to **Maps** > **Network Topology**.

Step 2 Click the **Circuits/VCs** tab, and select the L3VPN service that you want to modify.

Step 3 Click the pencil (**Modify**) icon.

Step 4 To modify the selected L3VPN, choose **Modify VPN** and click **Next**.

The Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN.

Step 5 If required, you can modify the **IP MTU** value.

Step 6 To modify the VRFs associated with the selected L3VPN, choose **Modify VRF** and click **Next**.

The Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN. Along with modifying existing VRF parameters, you can also associate new Route Target values to the VRF.

While modifying VRFs, you cannot modify the QoS profiles associated with the UNIs, however, you can modify the QoS policies associated with the service endpoints.

Note You cannot modify the VRF name and device associated with the selected L3VPN.

Step 7 Make the required changes and click **Submit** to preview the configuration that will be deployed to the device.

Note When you modify a VPN, you cannot change the VRFs associated with the VPN. To modify the VRFs, see Add and Copy VRFs to an L3VPN Service, on page 572.

Step 8 Review your changes and click **Deploy** to deploy your changes to the device.

In case of a deploy failure on even a single device that is part of the service, the configuration is rolled back on all devices participating in the service.

Step 9 To verify that your changes were saved, view the L3VPN service details. See View L3VPN Service Details, on page 568.

Add and Copy VRFs to an L3VPN Service

Using Cisco EPN Manager you can create and associate new VRFs to existing L3VPN services. You can also copy the route target and other details from existing VRFs to create new VRFs for the L3VPN service.

To associate new VRFs with an L3VPN service:

Step 1 Navigate to **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Circuits/VCs** tab and select the L3VPN service to which you want to associate new VRFs.

You can also access the L3VPN Provisioning wizard by choosing **Configuration > Network > Service Provisioning**.

Step 3 Click the pencil (**Modify**) icon.

The L3VPN Provisioning wizard is displayed.

Step 4 Select **Add VRF** and click **Next**.

Step 5 Click the **+** icon to add the new VRF details manually. To auto populate the VRF details, click the device on the map to select it. The device details and a new name for the VRF are automatically populated on the VRF's page.

Step 6 You can copy VRF details from an existing VRF by clicking the **Copy From** drop-down list and selecting the required VRF.

Only those VRFs that are associated with the selected L3VPN are displayed along with the VRFs route target, and route redistribution details.

Step 7 Otherwise, manually specify the details of the VRFs that you want to add to the selected VPN service. For more information about the different VRF parameters, see, Create and Provision a New L3VPN Service.

Step 8 Make any required changes such as adding endpoint and BGP neighbor details and click **Submit**.

Step 9 Preview the configuration that is to be deployed to the device, make the required changes, and click **Deploy** to deploy the changes to the device.

To verify that your changes were deployed, view the selected L3VPN service's details. See View L3VPN Service Details.

For more information on modifying and deleting L3VPN services, see Delete an L3VPN Service Endpoint, on page 654 and Modify L3VPNs and VRFs, on page 571.

Provision Circuit Emulation Services

Summary of Cisco EPN Manager CEM Provisioning Support

Cisco EPN Manager supports the provisioning of Circuit Emulation (CEM) services. CEM provides a bridge between the traditional TDM network and the packet switched network (PSN). It encapsulates the TDM data into packets, provides appropriate header, and send the packets through PSN to the destination node. For more information, see Supported Circuit Emulation Services, on page 492.

You can also assign a MPLS TE tunnel to a CEM service to allow the CEM service to traverse through the network. Use the **Preferred Path** drop-down list in the Provisioning Wizard to assign a MPLS TE tunnel for a CEM service. For more information, see CEM Service Details References, on page 575.

Note Provisioning of CEM services will fail if the tunnel selected in preferred-path is not having sufficient available bandwidth.

Prerequisites for CEM Provisioning

The following prerequisites must be met before you can provision a CEM service:

- IP/MPLS connectivity must be enabled on the originating and terminating endpoints in a CEM service.
- CEM configurations such as loopback interface and ACR groups must be configured on the devices that will be used in the CEM service. For more information, see Configure Circuit Emulation , on page 321.

- Inventory collection status for the devices on which the CEM service will be provisioned must be *Completed*. To check this, go to **Inventory** > **Device Management** > **Network Devices**, and look at the status in the **Last Inventory Collection Status** column.
- Optionally, customers can be created in the system so that you can associate a CEM service to a customer during the service creation and provisioning process. From the left sidebar, choose **Inventory** > **Other** > **Customers** to create and manage customers.

Create and Provision a New CEM Service

The process of creating and provisioning a CEM service in Cisco EPN Manager involves:

- Specifying endpoints of the CEM service.
- Defining the attributes that influence how traffic that is delivered over the CEM service and through its endpoints will be treated.

Before you begin

For information about the prerequisites that must be met before you can provision a CEM service, see Prerequisites for CEM Provisioning, on page 573.

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which you want to create the CEM service.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Circuit Emulation**.

Step 7 From the **Service Type** drop-down list, choose the required CEM service type depending on the rate at which you want the circuit to transmit the data. For a list of CEM service types that Cisco EPN Manager supports, see Supported Circuit Emulation Services, on page 492.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the **Customer Service Details** page.

Step 10 (Optional) Select the customer for whom the EVC is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then go to the Provisioning Wizard to start provisioning the CEM service.

Step 11 Check the **Activate** check box to activate the interface associated with the service that you are provisioning.

Step 12 Enter the service name and its description.

Step 13 In the **Deployment Action** field, specify what you want to do when the CEM service creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

If you choose Deploy, then click one of the following deployment options:

- Deploy Now—Directly deploys the provisioning order
- Deploy Later—Saves the created provisioning order and deploys the same order at later period of time.

- Schedule Deployment—Schedules the provisioning order and to be deployed at the scheduled time. If you click this **Schedule Deployment** radio button, specify the following:
  - Deploy Schedule Time—Specify a schedule time for deployment of provision order.
  - Server Time—Displays the current server time.

Step 14 Click **Next**, and then enter the A End and Z End configurations, and the transport settings for the CEM service. See CEM Service Details References, on page 575 for descriptions of the fields and attributes.

Step 15 If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, check the **Unmanaged Device** check box and provide information for the unmanaged device. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 609 for more information.

Note The **Unmanaged Device** check box is available only in the Z End Configurations page.

Step 16 (Optional) If you want to append a template with additional CLI commands that will be configured on the devices participating in the service, do so in the **Template Details** page. See Extend a Circuit/VC Using Templates, on page 609 for more information.

Step 17 When you have provided all the required information for the service, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The CEM service should be added to the list in the Circuits/VCs pane in the **Network Topology** window, to check the provisioning state, click on the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view. Also, you can view the saved provisioning job in the Planned Circuits/VCs tab from **Inventory** > **Other** > **Circuits/VCs & Network Interfaces** > **Planned Circuits/VCs**.

CEM Service Details References

The following table lists and describes the attributes that define the CEM service types.

Table 46: Circuit Section Reference—CEM Service Types

Attribute	Description
A End and **Z End Configurations**	
Device	Name of the source and destination devices in the CEM service.
Working Path and Protecting Path	
Port Name or Interface Name	Name of the interface on the source and destination devices in the CEM service. You can choose either the port name or the port group. When you choose the port name under the **Protecting Path** area, the unidirectional path switched ring (UPSR) protection mechanism is enabled. When you choose the port group under the **Protecting Path** area, the Automatic Protection Switching (APS) protection mechanism is enabled. For more information about how to configure protection groups, see Configure APS or MSP and UPSR or SNCP Protection Groups, on page 327.

Attribute	Description
Higher Order Path	When a SONET/SDH line is channelized, it is logically divided into smaller bandwidth channels called higher order paths (HOP) and lower order paths (LOP). HOP or synchronous transport signal (STS) path is used to transport TDM data of higher bandwidth. HOPs can also contain LOPs within it. Select the path and path mode available for the CEM service.
Lower Order Path	LOPs or virtual tributary (VT) path is used to transport TDM data of lower bandwidth.
DS0 Time Slot	Choose one or more time slots available in the DS0 group. **Note** This field is available only if you select **DS0** in the **Service Type** field.
Clocking The nodes in a network may be at different clock rates. Differences in timing at nodes may cause the receiving node to either drop or reread information sent to it. Clocking is essential to synchronize all nodes to the same clock rate. For more information about clocking, see Configure Clocking for CEM, on page 330.	
Clock Source	Enables to recover the clock rate from single source so that all nodes can be synchronized at the same clock rate. Values are: • Internal – Clock rate recovered from the host. • Line – Clock rate recovered from the SONET/SDH line. • Adaptive Clock Recovery – Clock rate is recovered based on the dejitter buffer fill level. Due to delay variations, the dejitter buffer fill levels keep varying continuously. The TDM service clock is recovered after filtering the variations. The accuracy of the recovered clock depends on the delay variations. • Differential Clock Recovery – Clock rate is recovered from a primary clock using Sync-E. For more information about how to setup the primary clock for your network, see Synchronize the Clock Using Sync-E, BITS, and PTP, on page 340.
QOS The list of profiles available for selection includes policy maps that were configured on the device and discovered by the system, as well as user-defined QoS profiles.	
Ingress QoS Profile	Select the ingress QoS policies that are configured on the A end and Z end devices.
Unmanaged Device Details **Note** The below fields are available only for Z End Configurations.	
Unmanaged Device	Check this check box to include a device that is not managed by Cisco EPN Manager and create partial service.
New Device	Check this check box to create a new unmanaged device.

Attribute	Description
Device	Choose an unmanaged device from the drop-down list. **Note** This field is available only when the **New Device** check box is unchecked.
Device Name	Enter a unique name for the new unmanaged device that you want to create. **Note** This field is available only when the **New Device** check box is checked. If the **New Device** check box is unchecked, the name of the unmanaged device that you chose in the **Device** drop-down list is populated in this field.
Device IP	Enter the IP address of the new unmanaged device that you want to create. **Note** This field is available only when the **New Device** check box is checked. If the **New Device** check box is unchecked, the IP address of the unmanaged device that you chose in the **Device** drop-down list is populated in this field.
LDP IP	Enter a valid LDP IP for the unmanaged device.
VC ID	Enter a unique Virtual Circuit (VC) ID for the unmanaged device.
Transport Settings	
Frame Type	This field is display-only and is auto-populated based on the CEM service type that you chose when creating the CEM service. The values are CESoPSN, SAToP, FRAMED_SAToP and CEP. For T1, T3, E1 and E3 CEM service types, choose the frame type as SAToP or FRAMED_SAToP. You can choose the frame type CEP for the service type E3 over E3 controllers. **Note** View the CLI changes for T1/T3 and E1/E3 services over SONET framed mode with SDH in the **Device Preview Config** after deployment of a CEM service. The FRAMED-SAToP frame type is supported on NCS42xx or ASR9xx device.
Payload Size	Number of bytes put into each IP packet. The valid range is 64 – 1312. The range will vary based on the device capability, level of support and the configured dejitter buffer size value.
Dejitter Buffer Size	Determines the ability of the emulated circuit to tolerate network jitter. The valid range is 1 - 32. The range will vary based on the device capability, level of support and the configured payload size value.
Idle pattern	Idle pattern to transmit the data when the service goes down. The valid range is 0x00 - 0xFF.
Dummy Mode	Enables you to set a bit pattern for filling in for lost or corrupted frames. The values are last-frame and user-defined.

Attribute	Description
Dummy Pattern	The bit pattern used for filling in for lost or corrupted frames. The valid range is 0x00 - 0xFF. The default is 0xFF. **Note** This field is enabled only if you choose the Dummy Mode as user-defined.
RTP Header Enabled	Check this check box to enable the Real-Time Transport Protocol (RTP) header for the CEM service.
RTP Compression Enabled	Check this check box to compress the IP header in a packet before the packet is transmitted. It reduces network overhead and speeds up the transmission of RTP.
Pseudowire Settings	
Preferred Path Type	Choose the Preferred Path Type as Bidirectional or Unidirectional.
Preferred Path	Select the MPLS bidirectional TE tunnel through which you want the CEM service to pass through. **Note** This field is available only if you selected **Bidirectional** as the Preferred Path Type.
Preferred Path (A-Z)	Select the required unidirectional tunnel through which you want the CEM service to travel from the A endpoint to the Z endpoint. **Note** This field is available only if you selected **Unidirectional** as the Preferred Path Type.
Preferred Path (Z-A)	Select the required unidirectional tunnel through which you want the CEM service to travel from the Z endpoint to the A endpoint. **Note** This field is available only if you selected **Unidirectional** as the Preferred Path Type.
Allow Fallback to LDP	Check this check box to ensure that the CEM service falls back to the default MPLS Label Distribution Protocol (LDP) when the selected preferred path goes down. **Note** This check box is available only when you select a valid MPLS TE tunnel in the **Preferred Path** field.
Send Control Word	Check this check box if you want a control word to be used to identify the pseudowire payload on both sides of the connection.
Internetworking Options	Choose an option if one of the endpoints in the EVC is an unmanaged device
Bandwidth (Kbps)	Enter the required bandwidth for the pseudowire.
PWID	Enter a presudowire identifier. This ID is displayed in the Pseudowire settings for point-to point services.

Modify a CEM Service

You can modify the CEM services that are created and deployed using Cisco EPN Manager.

Before you begin

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, select the location in which you want to modify the CEM service, and then click **Load**.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs** tab and select the CEM services that you want to modify.

Step 5 Click the pencil (Modify) icon.

The Modify CEM window appears. You can only modify the **Z Endpoint** details.

Step 6 To modify the **Device**, you can select a device from the **Device** drop down list.

Step 7 To modify the **Working Path**, you can select the **Interface Name** from the drop down list.

Step 8 To modify the **Higher Order Path**, you can select the **Available Paths** and **Path Mode** from the drop down list.

Step 9 To modify the **Lower Order Path**, you can select the **Available Paths** from the drop down list.

Step 10 Make the required changes and click **Submit** to preview the configuration that will be deployed.

Step 11 Review your changes and click **Deploy** to deploy your changes to the device.

Save and Schedule a Provisioning Order

When you create, modify, or delete provisioning services such as Circuits/VCs, MPLS tunnels or L3VPN service technologies you can either preview or deploy services. You can choose deploy options such as Deploy Now, Deploy Later, and Schedule Deployment before you save or schedule a provisioning order.

View the saved provisioning orders in the **Planned Circuits/VCs** tab and if necessary you can modify the planned services or create succeeded services. Following are some of the limitations:

- If the planned version exists all modify and delete operations for live circuits are disabled. Also, you cannot amend services under **Inventory** > **Circuits/VCs&Network Interfaces** for planned order. For more information, see the What to do Next section.
- If you edit the order from Planned circuits, Cisco EPNM allows modification against planning.
- The delete action from Planned circuits deletes the planned service that is reverted to the last attempted provisioned version. For scheduled orders, if the time is updated from the Job dashboard then the same time will not reflect in the **Planned Circuits**.

To save and schedule deployment:

Step 1 Create a planned provisioning order through one of the following paths:

Choose **Maps** > **Topology Maps** > **Network Topology**

—Or—

Inventory > **Circuits/VCs&Network Interfaces**

Step 2 Repeat steps 2 through 12 from the Provision Circuits/VCs in Cisco EPN Manager topic.

Step 3 To save and schedule deployment:

a) Under the Deploy area, click the **Deploy Later** radio button to save the provisioning order.

b) Under the Deploy area, click the **Schedule Deployment** radio button to save the order for future deployment at the designated time provided by you. Specify the following values.

- **Deploy Schedule Time**—Specify a schedule time for deployment of a provisioning order.
- **Server Time**—Displays the current server time.

c) Click **Next** to choose the endpoints and define the attributes based on the technology you have selected.

d) Click **Submit** Depending on the deployment action you have chosen, the relevant action will be performed. That is, if you have chosen to preview the configuration, the preview page will be displayed where you can view the configurations, and then click **Deploy**. If you have chosen to deploy, the configurations will be directly deployed to the relevant devices. After you receive the Deployment Saved/Schedule successful message, click **Close**.

Step 4 In the left pane, click the CircuitVCs hyperlink. The Locations/All Locations/Unassigned extended view window appears.

Step 5 Click the **Planned Circuit VC** tab to view the newly created provisioning service details. The status of the newly created provisioning service is displayed as "Create Planned". View the deployment schedule time, type and name of service to be provisioned, customer name and the last modified date and time. If required, you can modify the service again. For the planned service you can perform multiple amends until deployment. The status will be displayed as "Modify Planned".

Note The **Planned Circuit /VCs** tab will be available only when you click the CircuitVCs from the **Maps** > **Topology** > **Network Topology**. For **Deploy Later** option the deployment schedule time is not displayed.

During multiple amends the latest version is captured. In due course, if there is a scheduled order and the latest version is set to deploy later then all the previous scheduled order will be deleted from the Job dashboard.

Step 6 Click the create planned order and then choose **Actions** > **Deploy** to directly deploy the service.

Step 7 (Optional) You can perform other actions, if required:

a) Click the + icon to create a new provisioning workflow.

b) Click **X** icon to delete the planned service. A successful or failure message is displayed at the bottom right corner of the window after the service is deleted.

c) Deploy Later service is deleted if **X** is clicked and no traces are saved in the EPNM about this planned undeployed service.

d) If a deployed scheduled service is deleted , the corresponding job and service is cleared.

Step 8 To view the Scheduled provisioning job choose **Administration** > **Dashboard** > **Job Dashboard**. The status is displayed as Scheduled and you can view the next start time of deployment and so on.

a) (Optional) Click the **Edit Schedule** to edit the schedule order.

- In the **Schedule** window, modify the schedule time and other details, if required.
- Click **Save** and return to the Job Dashboard window.

b) (Optional) Click the **X** icon to delete the job.

After the job is successfully deployed, the entry is listed in the job dashboard. For Deploy Later option, a job will not be created as the time is not defined.

What to do next

Choose **Inventory** > **Circuits/VCs&Network Interfaces** to view the Planned Circuits/VCs. You can create a new provisioning workflow, deploy the existing service or amend the service for a given provisioning order. After the deployment is successful the provisioning order entry is cleared from the **Planned Circuits/VCs** tab.

Note View the deployed Circuit /VCs in the **Cirvuits/VCs** tab and the Planned Circuits in the **Planned Circuit /VCs** tab.

You cannot perform modify or delete operation for live Circuits/VCs. This is because you have to first clear the planned version before making further amends to the deployed version. Click the **Planned Circuits/VCs** to make amends to the selected Circuits/VCs or deploy the planned version.

Delete Operation

When you delete the planned version, a successful message or failure message is displayed at the bottom right corner of the window. After the service is deleted in the **Circuit/VCs** tab the status is displayed as "Modify Plan Canceled," and "Delete Plan Canceled".

If you delete a service from the **Planned Circuit/VCs** tab, the associated UNIs will also be deleted from the **Network Interfaces** tab. The deleted UNIs will be available for reuse.

Preview Config

During creation of new provisioning Circuits/Vcs, if the **Deployment Action** is chosen as **Preview** then you have the option to choose either **Deploy Now** or **Deploy Later** or **Schedule Deployment** in the **Deploy** page.

View Network Interfaces

In the **Circuits/VCs** tab, click Network Interfaces to view network interface details for provisioning services. You can modify or delete an interface using a Wizard.

Provision an EM-Voice CEM Service

On EM IM, ports 0-3 form one group and ports 4 and 5 form another group, the applicable EM types for each of these groups will now be reflected in EPNM during service provisioning, and you can view the list of applicable type for every port.

To provision a CEM service for the selected service type EM-Voice:

Step 1 In the left pane, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location where you want to create the CEM service.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

You can also access the Provisioning wizard by choosing **Configuration** > **Network** > **Service Provisioning**.

Step 6 From the **Technology** drop-down list, choose **Circuit Emulation**.

Step 7 From the **Service Type** drop-down list, choose **EM-Voice** to transmit the data. For a list of CEM service types that Cisco EPN Manager supports, see Supported Circuit Emulation Services, on page 492.

Step 8 If you have defined profiles to set the attributes of the different services, select the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** and then enter the service name and its description.

Step 10 Click **Next** and then enter the A End configurations for the CEM service. See CEM Service Details References, on page 575 for descriptions of the fields and attributes.

a) From the **Port Name** drop-down list, choose the interface name. Based on the configurations on the device, the ports are listed and you can view the list of applicable type for every port.

b) From the **EM Type** drop-down list, choose the type that can be configured on a port.

Note The **Type** will be listed based on the Interface name and **Applicable Type** that you have chosen in the **Port Name** field.

Step 11 Click **Next**, and then enter the Z End configurations for the CEM service.

Note EM Type must be same as A Endpoint EM Type.

Step 12 Click **Submit** to push the configuration to the device. If you chose to see a preview of CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

Provision MPLS Traffic Engineering Services

Summary of Cisco EPN Manager MPLS TE Provisioning Support

Cisco EPN Manager supports the provisioning of MPLS Traffic Engineering services. MPLS TE enables an MPLS backbone to replicate and expand the TE capabilities of Layer 2 over Layer 3. MPLS TE uses Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP) across the backbone. For more information, see Supported MPLS Traffic Engineering Services, on page 495.

MPLS TE Service Provisioning Features

Cisco EPN Manager supports the following MPLS TE features:

- Support for explicit routing, constraint-based routing, and trunk admission control.
- Provision for path protection mechanism against link and node failures.
- Usage of Resource Reservation Protocol (RSVP) to establish and maintain label-switched path (LSP).
- Ability to advertise TE links using OSPF and ISIS.

Following are the MPLS TE limitations in Cisco EPN Manager:

- MPLS TE tunnel is supported only on NCS 4206, 4216 devices, NCS4K, NCS 5500, ASR9k, and ASR9XX. However, inventory support is provided for NCS 4201 and NCS 4202.
- OSPF and ISIS are supported as the IGP for implementing MPLS TE.
- Wrap protection, BFD and fault-oam are not supported in NCS5500 device.
- MPLS TE attributes are available and populated in database only if the attributes are provisioned through the Cisco EPN Manager web-interface.

Note For the list of devices that support the provisioning of MPLS TE tunnel, see Cisco Evolved Programmable Network Manager Supported Devices

Create and Provision an MPLS TE Layer 3 Link

To provision an MPLS TE Layer 3 Link:

Before you begin

For information about the prerequisites that must be met before you can provision an MPLS TE Layer 3 Link, see Prerequisites for Provisioning an MPLS TE Service, on page 589.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**

Step 2 Click **Device Groups**, and then select the location in which you want to create the MPLS TE Layer 3 Link.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Step 6 From the **Technology** drop-down list, choose **MPLS TE**. Cisco EPN Manager displays a list of relevant service types in the **Service Type** area.

Step 7 In the **Service Type** area, choose **Layer 3 Link**.

Step 8 If you have defined profiles to set the attributes of the different services, choose the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the **Link Settings** page.

Step 10 Enter a name and description for the layer 3 link.

Step 11 Choose the **A End Device**, **A End Interface**, **Z End Device**, and **Z End Interface** fields using one of the following ways:

- Click a link on the map to automatically populate the **A End Device**, **A End Interface**, **Z End Device**, and **Z End Interface** fields.
- Click a device node on the map to automatically populate the **A End Device** field. If the A End Device is connected to only one device, the **Z End Device** field is populated automatically. If the **A End Device** is connected to more than one device, you must choose the **Z End Device** manually.

Step 12 Enter the IP address and mask for the A End and Z End devices.

Step 13 Choose an L2 Discovery Protocol from the following options:

- NONE—No L2 discovery protocol to be enabled for the layer 3 link.
- CDP—Cisco Discovery Protocol to be enabled for the layer 3 link to facilitate communication between Cisco devices connected to the network.
- LLDP—Link Layer Discovery Protocol to be enabled for the layer 3 link to support non-Cisco devices and to allow for interoperability between other devices that supports the IEEE 802.1AB LLDP.
- ALL—Both, CDP and LLDP to be enabled for the layer 3 link.

Step 14 Choose the required routing protocol for the layer 3 link. The values are BGP, ISIS, and OSPF. For information about how to configure the routing protocols, see Configure Routing Protocols and Security, on page 413

Step 15 (Optional) Enter a Link VLAN ID for the layer 3 link.

Step 16 (Optional) Check the **Enable MPLS TE** check box to support MPLS TE on the layer 3 link that you are provisioning.

Note This check box is available only when you choose OSPF or ISIS as your routing protocol.

Step 17 Click **Next**, and then enter the A End and Z End details. See Field References for A End Details and Z End Details in MPLS TE Layer 3 Link, on page 584 for descriptions of the fields and attributes.

Step 18 In the **Deployment Action** field, specify what you want to do when the MPLS layer 3 link creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

Step 19 Click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The service should be added to the list in the **Circuits/VCs** tab in the Network **Topology** window. To check the provisioning state, click the i icon next to the circuit/VC name to see the Circuit/VC 360 view.

Field References for A End Details and Z End Details in MPLS TE Layer 3 Link

The following table lists and describes the attributes that define the MPLS TE Layer 3 Link.

Table 47: Field References for A End and Z End Details—MPLS TE Layer 3 Link

Attribute	Description	Available when the routing protocol is:
Same as A End	Check this check box if you want to have the same routing and MPLS-TE configurations for both A end and Z end devices. **Note** This check box is available only in the Z End Details page of the Provisioning Wizard.	BGP, ISIS, and OSPF
BGP AS Number	Choose the unique BGP autonomous system number assigned for your network.	BGP
Route Policy	Choose the routing policy to control which routes the BGP stores in and retrieves from the routing table.	BGP

Attribute	Description	Available when the routing protocol is:
Route Reflector Client	Check this check box to configure the BGP neighbor as the route reflector client for the local route reflector to advertise the available routes.	BGP
Use AIGP	Check this check box to use the Accumulated Interior Gateway Protocol (AIGP) metric attribute for the layer 3 link. The AIGP is the BGP attribute that carries the accumulated end-to-end metrics for the paths in the network.	BGP
Update Source	Choose the required source interface. **Note** This field is available only when the **Use AIGP** check box is unchecked.	BGP
ISIS Process ID	Choose an ISIS routing process ID that is available to both A end and Z end devices. For information about how to configure an ISIS process, see Configure an IS-IS, on page 417.	ISIS
Network	The network ID is automatically populated based on the ISIS process ID selected.	ISIS
Circuit Type	Choose the type of adjacency required for the layer 3 link from the following options: • NONE—No adjacency is established. • Level-1—Establishes a level 1 adjacency if there is at least one area address in common between the selected device and its neighbors. • Level-2-only—Establishes a level 2 adjacency on the circuit. If the neighboring device is a level 1 only device, no adjacency will be established. • Level-1-2—Establishes a level 1 and 2 adjacency if the neighbor is also configured as a level 1-2 device and there is at least one area in common. If there is no area in common, a level 2 adjacency is established.	ISIS
Level 1 Metric	Enter the metric that must be used in the SPF calculation for Level 1 (intra-area) routing. **Note** This field is available only when you choose the **Circuit Type** as **Level-1** or **Level-1-2**.	ISIS

Attribute	Description	Available when the routing protocol is:
Level 2 Metric	Enter the metric that must be used in the SPF calculation for Level 2 (inter-area) routing. **Note** This field is available only when you choose the **Circuit Type** as **Level-2** or **Level-1-2**.	ISIS
OSPF Process ID	Choose an OSPF routing process ID. For information about how to configure an OSPF process, see Configure OSPF, on page 419. **Note** You cannot modify the OSPF routing process for the Z end device.	OSPF
OSPF Area	Enter the area in which you want to deploy the OSPF routing process.	OSPF
Metric	Enter the routing metric used by the OSPF routing process.	OSPF
BFD Template	Choose a BFD template for the layer 3 link. A BFD template defines the set of configurable parameters used by a BFD session. These include the transmit and receive timers used for BFD control and echo packets, the transmit timer interval used when the session is providing a CV function, the multiplier value, and the echo-receive interval. **Note** BFD Template is applicable for IOS-XE devices.	ISIS, and OSPF
BFD Min Interval	Enter the minimum control packet interval for BFD sessions for the corresponding BFD configuration scope. **Note** This field is available only if you have not chosen the **BFD Template**.	BGP, ISIS, and OSPF
BFD Multiplier	Enter the BFD multiplier. This value along with the BFD minimum interval is used to determine the intervals and failure detection times for both control and echo packets in asynchronous mode on bundle member links. **Note** This field is available only if you have not chosen the **BFD Template**.	BGP, ISIS, and OSPF

Attribute	Description	Available when the routing protocol is:
BFD Fast Detect	Check this check box to quickly detect failures in the path between adjacent forwarding engines. **Note** This is applicable only for IOS-XR devices.	BGP, ISIS and OSPF
Authentication Mode	Choose the required authentication mode used to send and receive ISIS packets. **Note** The authentication fields are available only when you select Cisco IOS XE devices. Available options are NONE, HMAC_MD5, and TEXT. By default, NONE is selected.	ISIS
Authentication Key Chain	Choose the authentication key chain. This enables authentication for routing protocols and identifies a group of authentication keys.	ISIS
Authentication for Send Only	Check this check box to perform authentication only for ISIS packets that are being sent. **Note** This is applicable only for IOS-XE devices.	ISIS
Password Type	Choose the password type as **Encrypted** or **Plain Text**.	BGP
Password	Type the desired password. Password is required to establish connection between two peers.	BGP
MPLS-TE		
Loopback Interface	Choose a loopback interface address for the layer 3 link. For information about how to configure a loopback interface, see Configure Loopback Interfaces.	ISIS and OSPF
Administrative Weight	Enter the MPLS TE tunnel metric with mode absolute.	ISIS and OSPF
TE Attributes	Enter the MPLS TE Link attribute to be compared with a tunnel's affinity bits during path selection.	ISIS and OSPF
Is Percentage	Check this check box to assign the bandwidth in percentage for the layer 3 link.	ISIS and OSPF

Attribute	Description	Available when the routing protocol is:
Global Bandwidth	Enter the regular TE tunnel bandwidth that will be reserved for the layer 3 link for CBR. For example, if you want to assign 10% as the global bandwidth for the layer 3 link, select the **Is Percentage** check box and enter the value 10 in the **Global Bandwidth** field. Whereas, if you want to assign 50 Kbps as the global bandwidth, uncheck the **Is Percentage** check box, choose Kbps from the **Bandwidth Unit** drop-down list, and then enter the value 50 in the **Global Bandwidth** field.	ISIS and OSPF
Subpool Bandwidth	Enter the subpool bandwidth that is reserved from the global pool bandwidth. For example, if you want to assign 10% as the subpool bandwidth for the layer 3 link, select the **Is Percentage** check box and enter the value 10 in the **Subpool Bandwidth** field. Whereas, if you want to assign 50 Kbps as the subpool bandwidth, uncheck the **Is Percentage** check box, choose Kbps from the **Bandwidth Unit** drop-down list, and then enter the value 50 in the **Subpool Bandwidth** field.	ISIS and OSPF
Auto Tunnel Backup	Check this check box to enable a router to dynamically build backup tunnels on the interfaces that are configured with MPLS TE tunnels.	ISIS and OSPF
Exclude SLRG for Backup Tunnel	Check this check box to enable the exclusion of SRLG values on a given link for the AutoTunnel backup associated with a given interface.	ISIS and OSPF
BFD Fast Detect	Check this check box to quickly detect failures in the path between adjacent forwarding engines.	ISIS and OSPF
QoS		
Ingress Policy	Select the ingress QoS policies that are configured on the A end and Z end devices.	BGP, ISIS, and OSPF
Egress Policy	Select the egress QoS policies that are configured on the A end and Z end devices.	BGP, ISIS, and OSPF
Additional Settings		
Enable MPLS TE	Check this check box to support MPLS on the layer 3 link that you are provisioning.	ISIS and OSPF

Attribute	Description	Available when the routing protocol is:
Enable SyncE	Check this check box to enable Synchronous Ethernet at the interface level for the layer 3 link. **Note** This is applicable only for IOS-XE devices.	BGP, ISIS, and OSPF

Prerequisites for Provisioning an MPLS TE Service

The following prerequisites must be met before you can provision an MPLS TE service:

- OSPF or IS-IS must be configured on the devices that participate on the MPLS TE service.
- LLDP / CDP must be enabled before provisioning MPLS TE L3 Link.
- All links that will be used for MPLS TE service provisioning must be TE enabled.
- The TE enabled links must be operationally up.
- The tunnel's source and destination nodes must be reachable.
- You can set up WAE parameters REST call from EPN Manager automatically.
- MPLS reachability must be set up between the devices. MPLS core network configuration must be set up.
- Inventory collection status for the devices on which the MPLS TE service will be provisioned must be Completed. To check this, go to **Inventory** > **Device Management** > **Network Devices**, and look at the status in the **Last Inventory Collection Status** column.
- Optionally, customers can be created in the system so that you can associate an MPLS TE service to a customer during the service creation and provisioning process. From the left sidebar, choose **Inventory** > **Other** > **Customers** to create and manage customers.

Create and Provision an MPLS TE Tunnel

To provision an MPLS TE tunnel:

Before you begin

For information about the prerequisites that must be met before you can provision an MPLS TE tunnel, see Prerequisites for Provisioning an MPLS TE Service, on page 589

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which you want to create the MPLS TE tunnel.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 Click the '+' icon to open the Provisioning Wizard in a new pane to the right of the map.

Step 6 From the **Technology** drop-down list, choose **MPLS TE**. Cisco EPN Manager displays a list of relevant service types in a **Service Type** area.

Step 7 In the **Service Type** area, choose **Unidirectional TE Tunnel** or **Bidirectional TE Tunnel**.

Step 8 If you have defined profiles to set the attributes of the different services, choose the required profile from the **Select Profile** drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 9 Click **Next** to go to the **Customer Service Details** page.

Step 10 (Optional) Select the customer for whom the service is being provisioned. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning wizard.

Step 11 Enter the service name and its description, and then enter the service details. See Field References for Service Details—MPLS TE Tunnel, on page 590.

Note
- If you do not provide a service name, Cisco EPN Manager assigns a service name in the following format:
  - If the source and destination devices have a common tunnel ID, the service name is assigned in the <SourceDeviceName>_<TunnelId>_<DestinationDeviceName> format.
  - If the source and destination devices have unique tunnel IDs, the service name is assigned in the <SourceDeviceName>_<ATunnelId>_<ZTunnelId>_<DestinationDeviceName> format.
- The signaled name of the tunnel must be unique across different devices in the system.

Step 12 Click **Next**, and then enter the tunnel creation parameters. See Field References for Tunnel Creation—MPLS TE Tunnel, on page 591 for descriptions of the fields and attributes.

Step 13 Click **Next**, and then enter the path constraint details. See Field References for Path Constraint Details—MPLS TE Tunnel, on page 597 for descriptions of the fields and attributes.

Step 14 Click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The service should be added to the list in the Circuits/VCs pane in the **Network Topology** window. To check the provisioning state, click the *i* icon next to the circuit/VC name to see the Circuit/VC 360 view.

Field References for Service Details—MPLS TE Tunnel

The following table lists and describes the attributes that define the service details for creating an MPLS TE tunnel.

Table 48: Service Details Section Reference—MPLS TE Tunnel

Attribute	Description
Activate	By default, this checkbox is checked. It enables the tunnel to be activated when deployed.
Enable FRR	Check this check box to enable the fast reroute feature that provides link and node protection for your MPLS TE tunnel. **Note** This check box is available only when you create a unidirectional TE tunnel.

Attribute	Description
Enable Auto Bandwidth	Check this check box to automatically assign maximum and minimum bandwidth to the TE tunnel based on the traffic.
Wrap Protection	Check this check box to detect midlink failure scenarios. **Note** This check box is available only when you create a bidirectional TE tunnel.
Enable Fault OAM	Check this check box to enable the fault OAM protocols and messages that support the provisioning and maintenance of MPLS TE tunnels. **Note** This check box is available only when you create a bidirectional TE tunnel.
Enable Autoroute	Check this check box to enable autoroute for the tunnel.
Enable BFD Settings	Check this check box to enable the Bidirectional Forwarding Detection (BFD) protocol. BFD provides fast forwarding path failure detection time and a consistent failure detection method.
Protection Type	Choose one of the following protection mechanisms for the TE tunnel: • Working—The tunnel has only a working path. • Working+Protected—The tunnel has a working and a protected path, wherein if the working path fails, the traffic flow is automatically routed to the protected path without the links going down. • Working+Restore—The tunnel has a working and a restore path, wherein if the working path fails, the link goes down and then the traffic flow is routed to the restore path. • Working+Protected+Restore—The tunnel has a working, protected, and restore path, wherein, if the working path fails, the traffic flow is routed to the protected path. If the protected path also fails, the link goes down and then the traffic flow is routed to the restore path.
Deployment Action	Choose one of the following options to specify what happens when the MPLS TE tunnel creation process is completed: • Preview—Previews the configurations that will be deployed to the relevant devices before the actual deployment. • Deploy—Deploys the configurations immediately upon completion.

Field References for Tunnel Creation—MPLS TE Tunnel

The following table lists and describes the attributes that define the MPLS TE tunnel creation.

Table 49: Tunnel Creation Section Reference—MPLS TE Tunnel

Attribute	Description
Create Tunnel	
Source	Source or A endpoint of the tunnel.
Source routing Process	OSPF or ISIS routing process that is TE enabled and configured on the source endpoint selected. You can determine the router ID and loopback address configured on the source endpoint based on the OSPF or ISIS routing process.
Destination	Destination or Z endpoint of the tunnel.
Destination Routing Process	OSPF or ISIS routing process that is TE enabled and configured on the destination endpoint selected. You can determine the router ID and loopback address configured on the destination endpoint based on the OSPF or ISIS routing process.
Tunnel Setting	
Global ID	The global ID assigned to both, source and destination endpoints. This ID must be the same to bind two unidirectional tunnels into a bidirectional TE tunnel. The default value is 0. **Note** This attribute is available only when you create a bidirectional TE tunnel. EPNM supports a global id only within the range of 1–2147483647.
Affinity Bits	The affinity bit determines the link attribute that the bidirectional TE tunnel uses when configuring the dynamic backup paths.
Affinity Mask	The affinity mask determines which link attributes the router must check. You can use affinity bits and affinity mask to include or exclude link attributes when configuring the dynamic backup paths. If a bit in the mask is 0, the value of the associated link attribute for that bit is irrelevant. In this case, the link attribute is excluded when configuring the dynamic backup paths. If a bit in the mask is 1, the value of the associated link attribute must match the affinity of the tunnel for that bit. In this case, the link attribute is included when configuring the dynamic backup paths.
Setup Priority	Setup priority assigned to an LSP for the unidirectional or bidirectional TE tunnels. Based on this priority, the LSP can determine which existing tunnels or LSPs with low priority can be blocked. Valid values are 0–7. A lower number indicates a higher priority. For example, an LSP with a setup priority of 0 can block any LSP with a setup priority 1–7. **Note** Setup priority cannot be higher than the hold priority.
Hold Priority	Hold priority assigned to an LSP for the unidirectional or bidirectional TE tunnels. Based on this priority, the LSP can determine whether it must be blocked by another signaling LSP with a high setup priority. Valid values are 0–7. A lower number indicates a higher priority. For example, an LSP with a hold priority of 0 cannot be blocked by another LSP.

Attribute	Description
Bandwidth Pool Type	Bandwidth pool used to manage the reservable bandwidth on each link for constraint-based routing (CBR) in MPLS TE. Values are: • Global – Regular TE tunnel bandwidth • Subpool – A portion of the global pool. The subpool bandwidth is not reserved from the global pool if it is not in use. Subpool tunnels require a higher priority than global pool tunnels. **Note** This field is available only when you uncheck the **Enable Auto Bandwidth** check box.
Bandwidth	Bandwidth for the bidirectional TE tunnel. You can choose the unit of the bandwidth from the drop-down list. The available units are Kbps, Mbps, and Gbps. For example, if you want to assign a bandwidth of 1000000 Kbps for the tunnel, enter the value as 1000 Gbps. **Note** This field is available only when you uncheck the **Enable Auto Bandwidth** check box.
Auto Bandwidth Max	Cisco EPN Manager automatically assigns the maximum bandwidth for the TE tunnel based on the traffic. However, you can change the bandwidth if required. You can choose the unit of the bandwidth from the drop-down list. The available units are Kbps, Mbps, and Gbps. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** screen.
Auto Bandwidth Min	Cisco EPN Manager automatically assigns the minimum bandwidth for the TE tunnel based on the traffic. However, you can change the bandwidth, if required. You can choose the unit of the bandwidth from the drop-down list. The available units are Kbps, Mbps, and Gbps. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** screen.
Bandwidth Change Frequency (Sec)	Enter the bandwidth change frequency in seconds. The valid range is 300–604800. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create tunnels.

Attribute	Description
Adjustment Threshold	Enter the bandwidth adjustment threshold in percentage to trigger an adjustment if the largest sample percentage is higher or lower than the current tunnel bandwidth. Adjustment threshold is the percentage of the current tunnel bandwidth and an absolute (minimum) bandwidth. Both the thresholds must be fulfilled for the automatic bandwidth to resignal the tunnel. The tunnel bandwidth is adjusted if the difference between the largest sample output rate and the current tunnel bandwidth is larger than the adjustment thresholds. The valid range for the tunnels that connect the Cisco IOS-XR devices is 1–100. The range for the tunnels that connect the Cisco IOS-XE devices is 1–99. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create tunnels.
Overflow Threshold	Enter the overflow threshold in percentage to trigger the overflow detection. It is the percentage of the actual signaled tunnel bandwidth. An overflow detection is triggered if the difference between measured bandwidth and actual bandwidth is larger than overflow threshold percentage for N consecutive times. This is also known as the overflow limit. The valid range for the tunnels that connect the Cisco IOS-XR devices is 1–100 and the range for the tunnels that connect the Cisco IOS-XE devices is 1–99. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create tunnels.
Overflow Limit	Enter the number of consecutive collection periods during which the difference between the measured bandwidth and the actual bandwidth of a tunnel can exceed the overflow threshold defined for the tunnel. The valid range is 1–10. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create tunnels.
Collect Bandwidth	Check this check box to collect the bandwidth information for the tunnel. **Note** This field is available only when you check the **Enable Auto Bandwidth** check box in the **Customer Service Detail** page when you create tunnels.
BFD Settings	
New BFD	This checkbox is selected by default when you select the **Enable BFD Settings** checkbox. Allows you to create a new BFD template for both bidirectional (Flex LSP) and unidirectional tunnels during provisioning.
BFD Template Name	Enter the name for the new BFD template.

Attribute	Description
BFD Template	Displays the selected BFD template name by concatenating the device name. For example, from A-End and/or Z-End devices. Choose an existing template from the existing template name and the related Min Interval and Multiplier range values are displayed by default. Alphabets, digits, and special characters _(underscore),-(hyphen),.(dot) are allowed, and BFD Template name should be fewer than 32 characters long. The BFD template name should not have .(dots) or digits or combination of digits and .(dots). **Note** This field is available only when you clear the **New BFD** checkbox.
Min Interval Multiplier	BFD uses intervals and multipliers to specify the periods at which control and echo packets are sent in asynchronous mode. It also detects their corresponding failure detection. A failure detection timer is started based on the following formula, where *I* specifies the minimum interval, and *M* is the multiplier: **`(I x M)`**. **Note** These fields are available only when you check the **Enable BFD Settings** check box and **New BFD** check box. Min Interval and Multiplier values are displayed for both new and existing BFD. For the existing BFD, you cannot edit the values.

Logic for BFD Template Usage

Use the BFD template configuration for unidirectional and FLEX LSP tunnels for XE devices. Use inline configuration for unidirectional and FLEX LSP tunnels for XR devices. EPNM provides an option either to create a new BFD template or to re-use an existing BFD template based on the following logic.

Note FLEX LSP tunnels are referred as Bidirectional Tunnels.

The following table lists the logic for using BFD template.

Table 50: Logic for BFD Template—MPLS TE Tunnel

Unidirectional	
Device Name Combination	**Configuration Logic Description**

XE-XE XE-XR	If you have chosen XE device as Source and destination (or XR device as destination), the logic works as a BFD Template configuration. To create a new BFD template: **1.** EPNM displays **New BFD** checkbox selected by default. **2.** Enter the name of BFD template. **3.** Enter the Min interval range value between 4-1000. **4.** Enter the Multiplier range value between 3-50. To re-use the existing BFD template: **1.** Clear the **New BFD** checkbox. **2.** From the **BFD Template** drop-down list, choose an existing BFD template. All existing BFD template names from A-End devices are listed. **3.** The Min Interval and Multiplier range values are displayed. **4.** Click **Submit**.
XR-XR XR-XE	If you have chosen an XR device as a source and destination (or XE device as destination), the logic works as an inline configuration. EPNM displays only **Min Interval** and **Multiplier** fields.
Bidirectional	
XE-XE	If you have chosen XE devices as source and destination, the logic works as a BFD Template configuration. To create a BFD template: **1.** EPNM displays **New BFD** checkbox selected by default. **2.** Enter the name of BFD template. **3.** Enter the Min interval range value between 4-1000. **4.** Enter the **Multiplier** range value between 3-50. To re-use the existing BFD template: **1.** Clear the **New BFD** checkbox. **2.** From the **BFD Template** drop-down list, choose an existing BFD template. All existing BFD template names from **A-End** and **Z-End** devices are listed. **3.** The Min Interval and Multiplier range values are displayed. **4.** Click **Submit**.

XE-XR	If you have chosen XE devices as Source and XR device as destination, the logic works as a BFD Template configuration. To create a new BFD Template: **1.** EPNM displays **New BFD** checkbox selected by default. **2.** Enter the BFD template name. **3.** Enter the Min interval range value between 4-1000. **4.** Enter the Multiplier range value between 3-10. To re-use the existing BFD template: **1.** Clear the **New BFD** checkbox. **2.** From the **BFD Template** drop-down list, choose an existing BFD template. This will list all existing BFD template names from A-End device. **3.** The **Min Interval** and **Multiplier** range values are displayed. **4.** Click **Submit**.
XR-XR	If you have chosen an XR device as a Source and destination, the logic works as an inline configuration. EPNM displays only **Min interval** and **Multiplier** fields.
XR-XE	If you have chosen an XR device as a source and XE device as a destination the logic works as a BFD Template configuration.. To create a new BFD template: **1.** EPNM displays **New BFD** checkbox selected by default. **2.** Enter the name of BFD template. **3.** Enter the Min interval range value between 4-1000. **4.** Enter the Multiplier range value between 3-10. To re-use the existing template: **1.** Clear the **New BFD** checkbox. **2.** From the **BFD Template** drop-down list, choose an existing BFD template. All existing BFD template names from **Z-End** device are listed. **3.** The **Min Interval** and **Multiplier** range values are displayed. **4.** Click **Submit**.

Field References for Path Constraint Details—MPLS TE Tunnel

The following table lists and describes the attributes that define the path constraint details for creating a MPLS TE tunnel.

Table 51: Path Constraint Details Section Reference—MPLS TE Tunnel

Attribute	Description
Path Type	Choose the required path for the TE tunnel. The values are **Working**, **Protected**, and **Restore**. Based on the value you choose in the **Path Type** field, the **Working Path**, **Protection Path**, and **Restore Path** field group is available.
Enable Lock Down	Select this check box if you do not want to reoptimize the working LSP.
Enable SRLG	Select the check box if you want to enable the SRLG. **Note** It can be configured only on the protect path.
Enable Sticky	Select this check box if you do not want to switch to a new LSP when there is a tunnel path change. **Note** It can be configured for the working path only when the lock down is enabled.
Enable Non-Revertive	Select this check box if you do not want to revert back to the initial working path from the protected path even if the working path is restored. **Note** It can be configured only on the protect path.
Type	Choose the type of working path or protected path for the tunnel. Values are **Dynamic** and **Explicit**.
New Path	Check this check box to create a new explicit working, protected, or restore path for the tunnel. **Note** All the below fields are available only when you select **Explicit** in the **Type** field.
Select Existing Path	Choose an existing explicit working, protected, or restore path for the tunnel. **Note** This field is available only when you uncheck the **New Path** check box.
Choose path from WAE server	Check this check box to specify the WAE networks and paths. **Note** This field is available only when you check the **New Path** check box. You can check or uncheck this check box if you have chosen **Dynamic** type and Path type as **Working**. It is recommended to check this check box if the explicit paths are to be read from the WAE server directly and not to be configured manually.
Select WAE Network	Click the down arrow to choose a WAE network from the dialog box. **Note** This field is available only when you check the **Choose path from WAE server** check box.

Attribute	Description
Select the WAE Path	Click the down arrow to choose an explicit path. **Note** This field is available only when you check the **Choose path from WAE server** check box.
Path Name	Enter a name for the explicit path that you are creating. In the **Working Path**, **Protection Path**, or **Restore Path** table, click the '+' button to add a new row to the table, and then select a MPLS-enabled device, an explicit path controller as the interface for the device, and a path constraint type. In the path table, you can select any MPLS-enabled device except the source and destinations devices. Cisco EPN Manager supports only strict path constraint type. **Note** This field is available only when you check the **New** check box.
Working Path LSP Attribute List, **Protection Path LSP Attribute List**, and **Restore Path LSP Attribute List** Based on the value you choose in the **Path Type** field, the respective field group is available. The LSP attributes that you define here are associated with the path option you selected in the **Path Type** field and these attributes are applicable for source and destination devices. **Note** The values that are defined for a specific path option will override the values specified at the interface tunnel level. For example, if you have defined the LSP attributes for the working path, these values will override the values that you defined in the **Tunnel Settings** section at the interface tunnel level, which is common for all the path options. For bidirectional tunnel, Working Path LSP attribute list can be configured only when **Enable Lock Down** check box is unselected.	
New LSP Attribute List	Check this check box to create a new LSP attribute list for the selected path type.
Existing LSP Attribute List	Choose an existing LSP attribute list for the selected path type. **Note** This field is available only when you uncheck the **New LSP Attribute List** check box.
LSP Attribute List Name	Enter a name for the LSP attribute list that you are creating. **Note** All the below fields including this field are displayed as read-only when the **New LSP Attribute List** check box in unchecked.
LSP Affinity Bits	Enter the LSP affinity bit that determines the link attribute that the bidirectional TE tunnel will use when configuring the backup paths (working, protected, or restore).
LSP Affinity Mask	Enter the LSP affinity mask that determines which link attribute the router must check when configuring the backup paths.

Attribute	Description
LSP Setup Priority	Enter the setup priority assigned to an LSP for the chosen path type. Based on this priority, the LSP can determine which existing tunnels or LSPs with low priority can be blocked. Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a setup priority of 0 can block any LSP with a setup priority between 1 and 7. **Note** LSP setup priority cannot be higher than the LSP hold priority. **Note** For Cisco IOS-XR devices, the **LSP Setup Priority** and **LSP Hold Priority** fields are not applicable.
LSP Hold Priority	Enter the hold priority assigned to an LSP for the chosen path type. Based on this priority, the LSP can determine whether it must be blocked by another signaling LSP with a high setup priority. Valid values are from 0 to 7. A lower number indicates a higher priority. For example, an LSP with a hold priority of 0 cannot be blocked by another LSP. **Note** For Cisco IOS devices, if you do not specify an LSP hold priority, Cisco EPN Manager takes the value specified in the **LSP Setup Priority** field. **Note** For Cisco IOS-XR devices, the **LSP Setup Priority** and **LSP Hold Priority** fields are not applicable.
LSP Record Route	Check the check box to record the route used by the LSP.

Provision Serial Services

- Prerequisites for Serial Circuits/VCs Provisioning, on page 600
- Create and Provision a New Serial Circuit/VC (RS232, RS422, and RS485), on page 601
- Create and Provision a New Serial Circuit/VC (Raw Socket), on page 604

Prerequisites for Serial Circuits/VCs Provisioning

Following are the prerequisites to provision a serial circuit/VC:

- Communication between devices must be set up before you can provision a serial circuit/VC.
- Inventory collection status for the devices on which the Serial circuits/VCs will be provisioned must be "Completed". To check this, go to **Inventory** > **Device Management** > **Network Devices**, and look at the status in the Last Inventory Collection Status column.
- Optionally, customers must be created in the system so that you can associate a circuit/VC to a customer during the circuit/VC creation and provisioning process. From the left sidebar, choose **Inventory** > **Other** > **Customers** to create and manage customers.

Create and Provision a New Serial Circuit/VC (RS232, RS422, and RS485)

To create a new serial circuit/VC:

Before you begin

For information about the prerequisites that must be met before you can provision a serial circuit/VC, see Prerequisites for Serial Circuits/VCs Provisioning, on page 600.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2 From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.

Step 3 Click the **Circuits/VCs** tab.

Step 4 From the **Circuits/VCs** pane toolbar, click the **+** (**Create**) icon.

The Provisioning Wizard opens in a new pane to the right of the map.

Step 5 Select **Serial** in the Technology drop-down list.

Step 6 In the Service Type list, select the type of serial service you want to create. For information about the serial service types that Cisco EPN Manager supports, see Supported Serial Services, on page 496.

Step 7 If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 8 Click **Next** to go to the Customer Service Details page.

Step 9 Select the customer for whom the circuit/VC is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customers** to create the customer in the system, and then restart the Provisioning Wizard.

Step 10 Check the **Activate** check box to specify whether the service must be in active state. The Active state enables traffic to pass through the circuit and automatically sets the service state of all the associated endpoints to True.

Step 11 Enter the service name and description.

Step 12 In the Deployment Action field, specify what you want to do when the circuit/VC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

Step 13 Click Next to go to the page in which you configure the endpoints. See Serial Service Details Reference, on page 602.

Step 14 If one of the endpoints is an interface on a device that is not managed by Cisco EPN Manager, provide information for the unmanaged device. See Provision a Circuit/VC with an Unmanaged Endpoint, on page 609 .

Step 15 Click Next to go to the Line Settings and Pseudowire Settings page. See Serial Service Details Reference, on page 602.

Step 16 Optional. If you want to append a template with additional CLI commands that will be configured on the devices participating in the circuit/VC, do so in the Template Details page. See Extend a Circuit/VC Using Templates, on page 609 for more information.

Step 17 When you have provided all the required information for the circuit/VC, click Submit. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window.

Serial Service Details Reference

The following table lists and describes the attributes that define the serial service type.

Table 52: Circuit Section Reference—Serial Service Type

Attribute	Description
A Endpoint and **Z Endpoint Configurations**	
Media Type	The media type selected for the serial interface service.
Device Name	Name of the source and destination devices in the serial service.
Port Name and Description	Name and description of the interface on the source and destination devices in the serial service.
Unmanaged Device Details **Note** The below fields are available only for Z Endpoint Configurations.	
Unmanaged Device	Check this check box to include a device that is not managed by Cisco EPN Manager and create partial service.
New Device	Check this check box to create a new unmanaged device.
Media Type	Choose either RS232 or RS422 as media type for an existing RS232 or RS422 service to create point-to-point RS232 to RS422 service. For example, at the A-end if there is an existing media type RS232, you can choose either RS232 or RS422 as media type at the Z-end for the point-to-point service configuration. **Note** You cannot modify a media type after it is created.
Device Name	Enter a unique name for the new unmanaged device that you want to create. **Note** This field is available as a drop-down list if you have unchecked the **New Device** check box. You can choose an unmanaged device as your Z endpoint.
Device IP	Enter the IP address of the new unmanaged device that you want to create. **Note** This field is available only when the **New Device** check box is checked. If the **New Device** check box is unchecked, the IP address of the unmanaged device that you chose in the **Device** drop-down list is populated in this field.
LDP IP	Enter a valid LDP IP for the unmanaged device.
VC ID	Enter a unique Virtual Circuit (VC) ID for the unmanaged device.
Line Settings	
Speed	The speed of the serial link in kilo bits per second.
Data Bits	The measurement of actual data per packet that is transmitted through the serial circuit/VC. The values are 5, 6, 7, and 8.

Attribute	Description
Stop Bits	Indicates the end of communication for a single packet. The values are 1, 1.5, and 2 bits. Since the data is clocked across the lines and each device has its own clock, it is possible for the two devices to become slightly out of sync. Therefore, the stop bits not only indicate the end of transmission but also provides the network with some lenience to synchronize the different clocks. The more bits that are used for stop bits, the greater the lenience in synchronizing the different clocks, but slower the data transmission rate.
Parity	Used to check errors in serial communication. The values are: • None—No parity defined for the circuit/VC. • Even— The serial port will set the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an even number of logic high bits. For example, if the data was 011, then for even parity, the parity bit would be 0 to keep the number of logic high bits even. • Odd— The serial port will set the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an odd number of logic high bits. For example, if the data was 011, then for odd parity, the parity bit would be 1, resulting in 3 logic high bits. • Mark— Sets the parity bit high. This allows the receiving device to know the state of a bit which enables the device to determine if noise is corrupting the data or if the transmitting and receiving devices' clocks are out of sync. • Space—Sets the parity bit low. This allows the receiving device to know the state of a bit which enables the device to determine if noise is corrupting the data or if the transmitting and receiving devices' clocks are out of sync.
Duplex Mode	Choose the required duplex mode for the serial service from the following options: • HalfDuplex—Supports communication in both directions between the endpoints, but not simultaneously. The transmission of data happens at one direction at a time. • FullDuplex—Supports simultaneous communication in both directions between the endpoints assuming that both endpoints support full duplex. If one side does not support full duplex, the port will be brought down. **Note** This field is available only for RS485 and RS422 service types. You can edit RS485 and RS422 service type details. This is because you can select Duplex mode between Half and Full for RS485 and RS422. However, you cannot edit RS232 service type details because for RS232 you can select only FULL Duplex mode.
Pseudowire Settings	
Preferred Path Type	Choose the Preferred Path Type as Bidirectional or Unidirectional.

Attribute	Description
Preferred Path	Select the MPLS bidirectional TE tunnel through which you want the serial service to pass through. **Note** This field is available only if you selected **Bidirectional** as the Preferred Path Type.
Preferred Path (A-Z)	Select the required unidirectional tunnel through which you want the serial service to travel from the A endpoint to the Z endpoint. **Note** This field is available only if you selected **Unidirectional** as the Preferred Path Type.
Preferred Path (Z-A)	Select the required unidirectional tunnel through which you want the serial service to travel from the Z endpoint to the A endpoint. **Note** This field is available only if you selected **Unidirectional** as the Preferred Path Type.
Send Control Word	Check this check box if you want a control word to be used to identify the pseudowire payload on both sides of the connection.

Create and Provision a New Serial Circuit/VC (Raw Socket)

To create a new serial circuit/VC with Raw Socket type:

Before you begin

For information about the prerequisites that must be met before you can provision a Raw Socket circuit/VC, see Prerequisites for Serial Circuits/VCs Provisioning, on page 600.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2 From the toolbar, click **Device Groups** and then select the group of devices you want to show on the map.

Step 3 Click the **Circuits/VCs** tab.

Step 4 From the **Circuits/VCs** pane toolbar, click the **+** (**Create**) icon.

The Provisioning Wizard opens in a new pane to the right of the map.

Step 5 Select **Serial** in the Technology drop-down list.

Step 6 In the Service Type list, select **Raw Socket**. For information about the Raw Socket circuits/VCs, see Supported Serial Services, on page 496.

Step 7 If you have defined profiles to set the attributes of the different services, select the required profile from the Select Profile drop-down list. See Create Circuit/VC Profiles , on page 607.

Step 8 Click **Next** to go to the Customer Service Details page.

Step 9 Select the customer for whom the circuit/VC is being created. If there are no customers in the list, go to **Inventory** > **Other** > **Customer** to create the customer in the system, and then restart the Provisioning Wizard.

Step 10 Enter the service name and description.

Step 11 In the Deployment Action field, specify what you want to do when the circuit/VC creation process is completed. You can either request a preview of the configurations that will be deployed to the relevant devices before the actual deployment or you can deploy the configurations immediately upon completion.

Step 12 Click **Next** to go to the Server Side Configuration page. See Raw Socket Service Details Reference, on page 605 for descriptions of the fields and attributes.

Step 13 Click **Next** to go to the Client Side Configuration page. Click the '+' icon in the Raw Socket Client table to add a new row for client side configuration. See Raw Socket Service Details Reference, on page 605 for descriptions of the fields and attributes.

Step 14 Optional. If you want to append a template with additional CLI commands that will be configured on the devices participating in the circuit/VC, do so in the Template Details page. See Extend a Circuit/VC Using Templates, on page 609 for more information.

Step 15 When you have provided all the required information for the circuit/VC, click **Submit**. If you chose to see a preview of the CLI that will be deployed to the devices, it will be displayed now and you can click **Edit Attributes** to change the attributes. Otherwise, the configurations will be deployed to the devices immediately.

The circuit/VC should be added to the list in the Circuits/VCs pane in the Network Topology window. From the Services tab, you can click the *i* icon that is present next to the newly created serial interface service and view the recently created endpoints on the server with both end points (that is server and its associated clients) in the **Circuit/VCs 360*** dialog box. Also, click the *i* icon next to the **Provisioning State** and view the configurations that are being pushed on to each end point.

Raw Socket Service Details Reference

The following table lists and describes the attributes that define the Raw Socket service type.

Table 53: Raw Socket Service Type—Server Side and Client Side Configurations

Attribute	Description
Server Settings and **Client Settings**	
Media Type	From the Media Type drop-down list, choose one of the following to configure a multipoint RS422 or RS4232 service, as part of cross circuit services. • RS232—If you choose RS232 option as media type, the SyncRS232 check box is available for Sync operation along with other configuration settings for serial interfaces. **Note** When you create a service (for example, Serial Raw Socket) with RS232, at the time of configuring the supported services both the end should have either RS232 or RS422, so that the corresponding server and its associated clients can be configured with only one media type at a time. You can configure these configuration settings on the Device and from the EPNM as well. • RS422—Allows you to configure client, server, and Packetization settings for RS 422 multipoint service.
Sync RS232	Check this check box to enable the synchronous mode of RS232 for the service.

Attribute	Description
Device Name	Name of the devices that act as a server and client in the Raw Socket service.
Port Name	Name of the interface on the server and client devices in the Raw Socket service.
Server Address and Server Port	The IP address and the port number of the server.
Allowed Sessions	To preconfigure a limit on the number of TCP raw-socket sessions per interface. Its default value is 32.
Client Address and Client Port	The IP address and the port number of the client.
Connection Idle Timeout	TCP session timeout setting for the Raw Socket service. If no data is transferred between the client and server over this interval, then the TCP session closes. The client then automatically attempts to reestablish the TCP session with the server.
VRF	Virtual Routing and Forwarding (VRF) interface through which the server and client are connected to transport the data. **Note** Ensure that the VRF definition is common for both server and client.
Speed	The speed of the serial link in kilo bits per second. This line setting is optional for Sync service settings.
Data Bits	The measurement of actual data per packet that is transmitted through the serial circuit/VC. The values are 5, 6, 7, and 8. This line setting is optional for Sync service settings.
Stop Bits	Indicates the end of communication for a single packet. The values are 1, 1.5, and 2 bits. This line setting is optional for Sync service settings.
Parity	Checks errors in serial communication. This line setting is optional for Sync service settings.
Duplex Mode	The duplex mode for the selected serial service. This line setting is optional for Sync service settings.
DTR	Choose one of the following options: • Used—Allows you to configure Data Terminal Ready (DTR) equipment from the customer end if there are no connected cables. • Not Used—Allows you not to configure Data Terminal Ready (DTR) equipment from the customer end if there are no connected cables. **Note** This option is available only if the SyncRS232 check box is selected.
Clock Rate	Choose the desired clock rate in bits per second (bps) for the service. The valid values are 48000 and 64000.
NRZI Encoding	Check this check box to enable the nonreturn-to-zero inverted (NRZI) encoding mechanism for the service.

Attribute	Description
Control Signal Transport	Check this check box to specify if the hardware control signals need to be sent to the remote PE.
Frequency	Enter the required frequency. The valid value is between 50 and 200. **Note** This field is available only when you check the Control Signal Transport check box.
Frame Pattern	Choose one of the required frame formats from the following options that will be used for internal signal transport: • BCN—Beacon • CFGR—Configure for test • NR0—Nonreserved 0 • NR1—Nonreserved 1 • NR2—Nonreserved 2 • NR3—Nonreserved 3
Connection Topology	The connection topology, either point-to-point or point-to-multipoint, for the service is displayed.
Packetization Settings	
Packet Length	The packet length that triggers the routing device (either a server or a client) to transmit the serial data to the peer. When the device collects the specified bytes of data in its buffer, it packetizes the accumulated data and forwards it to the Raw Socket peer.
Fragment Off	Check this check box to disable the frame relay fragmentation for this service.
Packet Timer	Specifies the amount of time in milliseconds, the device (either server or client) waits to receive the next character in a stream. If a character is not received by the time the packet timer expires, the data the device has accumulated in its buffer is packetized and forwarded to the Raw Socket peer.
Special Char	A character that triggers the device (either server or client) to packetize the data accumulated in its buffer and send it to the Raw Socket peer. When the specified special character is received, the device packetizes the accumulated data and sends it to the Raw Socket peer.

Create Circuit/VC Profiles

Profiles contain sets of attributes specific to different types of circuits/VCs. Once a profile is created, you can select it during circuit/VC creation. When a profile is selected, the Provisioning Wizard is populated with profile attributes. You must define the endpoints of the service and make changes before provisioning the circuit/VC, if necessary.

The types of profiles you can create mirror the types of circuits/VCs that can be provisioned.

Each profile is given a unique name, so you can create multiple profiles per circuit/VC type, depending on your needs.

To create a profile:

Step 1 Choose **Inventory > Other > Profiles** in the left navigation pane. The **Profiles** window opens, showing a table of existing profiles (if any). You can select a profile in the table to edit or delete it.

The Profiles window displays the attribute information of existing profiles, which includes name, description, profile ID, technology, Qualifier (non-editable, read-only parameter that helps differentiate between the OCH-Trail circuits types, mostly applicable for L0 circuits), and so on.

Step 2 Click **Create**.

Step 3 In the Create Profile wizard, provide a unique name for the profile and enter a description.

Step 4 Select the required technology type from the **Technology** list, for example, **Carrier Ethernet**. The relevant service types for the selected technology are displayed.

Step 5 Select the required service type.

For example, for L3VPN services, choose **Unicast** to create a profile that helps prepopulate values for most L3VPN service creation fields or choose **IPSLA Operations** to create a profile with IP SLA specific options for the L3VPN service.

Step 6 Click **Next** to go to the attribute definition page and define the attributes for the selected service type. The attributes in the profile are the same as the attributes in the Provisioning Wizard, and they are described in the following reference sections:

Information on Ethernet VCs attributes is provided in these topics:

- For attributes relating to the service itself, see Service Details Reference, on page 515.
- For attributes specific to the UNI, see New UNI Details Reference, on page 516.
- For attributes relating to the UNI as it operates within the service, see UNI Service Details Reference, on page 517.
- For UNI attributes, see Configure a Device and Interface To Be a UNI, on page 520.
- For ENNI attributes, see Configure a Device and Interface To Be an ENNI, on page 521.

Information on OCH and OTN attributes is provided in Circuit Section Reference for OCH Circuit Types, on page 531 and Circuit Section Reference for OTN Circuit Types, on page 545.

Information on L3VPN attributes is provided in Create and Provision a New L3VPN Service, on page 556 and View L3VPN Service Details, on page 568.

Step 7 Click **Save** when you have defined the attributes. The profile will be added to the table in the Profiles window.

Create Customers

Customers must be created in the system so that they are available for selection during the circuit/VC provisioning process.

To create a customer:

Step 1 From the left sidebar, choose **Inventory** > **Other** > **Customers**.

Step 2 Click **Create Customer**.

Step 3 Enter the name of the customer and a description (optional).

Step 4 Click **OK**. The customer is now added to the table of customers. You can select a customer to edit or delete it.

Provision a Circuit/VC with an Unmanaged Endpoint

You can create and provision a circuit/VC even if one or more of the endpoints is a device that is not managed by Cisco EPN Manager. The Provisioning Wizard allows you to identify an endpoint device as "unmanaged" and to provide information about that device so that the system can create the circuit/VC. Once you identify the unmanaged device, it will be available in the system in the Unmanaged Devices group and can be used for other services.

Step 1 Start the circuit/VC creation process for the required technology, as described in Provision Circuits/VCs, on page 499.

Step 2 For a point-to-point EVC and a CEM service:

a) When defining the Z endpoint, select the **Unmanaged Device** check box. The Unmanaged Device Details panel opens.

b) If the unmanaged device has already been identified in the system, deselect the **New Device** check box and select the required device from the list. If you are identifying a new unmanaged device, provide the device name, IP address, and LDP IP. The LDP IP is used as the neighbor address of the pseudowire on the managed device.

Step 3 For a point-to multipoint or multipoint -to-multipoint EVC: In the Unmanaged UNI page, click the Plus icon in the table to add a row and then define the Unmanaged Device Details and Service Endpoint details for the selected row.

Step 4 Complete the circuit/VC creation and provisioning process for the required technology, as described in Provision Circuits/VCs, on page 499.

Extend a Circuit/VC Using Templates

When you create and provision a circuit/VC, Cisco EPN Manager configures a set of CLI commands on the participating devices. If you need to configure additional commands on the same devices, you can create a template containing these commands and you can include it during the circuit/VC creation process. This effectively extends the circuit/VC beyond what is configured by Cisco EPN Manager. This functionality is available in the provisioning wizard but it is dependent on the template being created prior to creating or modifying the circuit/VC.

Extending a circuit/VC using CLI templates involves the following steps:

1. Create the CLI template using blank templates or existing templates. See Create a New CLI Configuration Template Using a Blank Template, on page 454 and Create a New CLI Configuration Template Using An Existing Template, on page 455.
2. Create/modify a circuit/VC and append the CLI template. See Provision Circuits/VCs, on page 499.

Step 1 Create the CLI template:

a) In the left sidebar, choose **Configuration > Templates > Features & Technologies**.
b) In the Templates panel, choose **CLI Templates > CLI**.
c) Provide identifying information for the new circuit and define the content of the template using CLI, global variables, and/or template variables. See Create a New CLI Configuration Template Using a Blank Template, on page 454 and Use Global Variables in a Template, on page 461.
d) Click **Save as New Template**.
e) The new CLI template is saved under **My Templates > CLI Templates (User Defined)**.

Step 2 Create/modify a service that includes the template you created (or a different template if relevant):

a) From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

b) Click the **Circuits/VCs** tab.
c) From the **Circuits/VCs** pane toolbar, either click the **+** (**Create**) icon or select a circuit and then click the pencil (**Modify**) icon.

The Provisioning Wizard opens in a new pane to the right of the map.

d) Start creating or modifying the required circuit or VC. See Provision Circuits/VCs, on page 499 and Modify a Circuit/VC, on page 644.
e) In the **Service Template** page, use the **Pre-Configuration** section if you want the template to be a prefix to the service configuration or use the **Post-Configuration** section if you want the template to be a suffix to the service configuration.
f) In the **Template** drop-down menu, select the required CLI template.

The same CLI template cannot be selected for both pre-configuration and post-configuration options.

g) In the **Template Usage** drop-down menu, select an option to indicate under what circumstances the CLI template should be configured on the devices. For example, if you select **Service Create Only**, the template CLI will only be configured on the devices when the service is created. It will not be configured when the service is modified.
h) Enter values for the template parameters. The parameters shown here depend on the variables that were defined for the template.
i) Click **Submit**.

Note By default, the selected CLI templates are associated with all devices that take part in the service. You cannot specifically choose the devices to be associated with the CLI templates.

Step 3 You can configure rollback templates for the configured templates. See Example Configuration: Rollback Template, on page 615.

Step 4 You can also configure interactive templates. See Example Configuration: Interactive Template, on page 616.

Example Configuration: Extend a Circuit/VC Using CLI Templates

Example Configuration 1: Extending an L3VPN service on a Cisco ASR 903 router device using a CLI template with Global and Template (Local) variables:

```
vrf definition Testdoc1
exit
```

```
vrf Testdoc1
  vpn id 36B:3
  address-family ipv4 unicast
    import route-target
      65:1
    export route-target
      65:1
  address-family ipv6 unicast
    import route-target
      65:1
    export route-target
      65:1
interface  GigabitEthernet0/0/0/11.2
  vrf   Testdoc1
  ipv4 address 4.5.7.8 255.255.255.0
  mtu 1522
router bgp 140
  vrf  Testdoc1
    rd auto
    address-family ipv6 unicast
    address-family ipv4 unicast
      redistribute static metric 54
    neighbor 3.4.6.8
      remote-as 21
      address-family ipv4 unicast
        exit
      exit
    exit
  exit
  interface GigabitEthernet0/0/6
  desc postconfig
  delay 5988
  mtu 436
  exit
```

Example Configuration 2: Extending a CEM service using a CLI template with a global variable and a template (local) variable:

```
#set($interfaceNameList = $gv.service-cem-cemInterfaceNameList.split(","))
#set($cemGroupNumberList = $gv.service-cem-cemGroupNumberList.split(","))
#set($count = 0)
#foreach($interfaceName in $interfaceNameList)
  interface $interfaceName
    service-policy input MainInterfacePolicy
    #if($count == 0)
      cem $cemGroupNumberList[0]
    #else
      cem $cemGroupNumberList[1]
    #end
        service-policy input servicePolicy
    #set($count = $count+1)
#end
```

Example Configuration 3: Extending a CEM service to configure QoS over CEM:

```
#set($count = 0)
#foreach($interfaceName in $gv.service-cem-cemInterfaceNameList)
interface $interfaceName
service-policy input MainInterfacePolicy
#if($count == 0)
cem $gv.service-cem-cemGroupNumberList[0]
#else
cem $gv.service-cem-cemGroupNumberList[1]
#end
```

```
service-policy input servicePolicy
#set($count = $count+1)
#end
exit
```

Example Configuration 4: Extending a Layer 3 Link service using a CLI template with a global variable and a template (local) variable:

```
##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
"MODIFY")
 ##XE DEVICE
 #if($variant=="IOS-XE")
 #if($gv.service-l3Link-routingProtocolName=="BGP")
   router bgp $gv.service-l3Link-routerProcessId
             address-family ipv4
           neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
    ##assume A End as remote building
           #if($gv.service-l3Link-isRouteReflectorClient=="TRUE" && $prefixListName!="" &&
 $gv.service-l3Link-endPointDesignation=="AEND")
    neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list send
                  neighbor $gv.service-l3Link-bgpNeighborName prefix-list $prefixListName
in
                  #elseif($gv.service-l3Link-isRouteReflectorClient=="TRUE" &&
$prefixListName!="" && $gv.service-l3Link-endPointDesignation=="ZEND")
    neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list receive
           #end
                exit
         exit
        #end

        #if($xeMTU!="" || $xeClnsMTU!="")
         interface $gv.service-l3Link-interfaceName
          #if($xeMTU!="")
              mtu $xeMTU
          #end
          #if($xeClnsMTU!="")
              clns mtu $xeClnsMTU
          #end
            exit
        #end

        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily !="" && $addressFamily=="vpnv4")
         router bgp $gv.service-l3Link-routerProcessId
          address-family $addressFamily
           neighbor $gv.service-l3Link-bgpNeighborName activate
     neighbor $gv.service-l3Link-bgpNeighborName send-community both
     #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
     neighbor $gv.service-l3Link-bgpNeighborName route-reflector-client
     #end
     bgp additional-paths install
     neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
           exit
         exit
 #end
 #end
 ##XR DEVICE
 #else

  #if($xrMTU!="")
  #if($gv.service-l3Link-subInterfaceName!="")
             interface $gv.service-l3Link-subInterfaceName
                  mtu $xrMTU
```

```
                exit
            #else
                interface $gv.service-l3Link-interfaceName
                     mtu $xrMTU
                exit
              #end
           #end

           #if($gv.service-l3Link-routingProtocolName=="BGP")
           #if($addressFamily !="" && $addressFamily=="vpnv4")
            router bgp $gv.service-l3Link-routerProcessId
             address-family $addressFamily unicast
         additional-paths receive
                exit
             neighbor $gv.service-l3Link-bgpNeighborName
              address-family $addressFamily unicast
                        #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
               route-reflector-client
                        #end
             aigp
                        #if( $routePolicyName!="")
             route-policy $routePolicyName in
                        #end
                       exit
                exit
              exit
           #end
           #end


 #end

##DELETE USE CASE
#elseif($gv.service-serviceOperationType == "DELETE")
 ##XE DEVICE
 #if($variant=="IOS-XE")

           #if($xeMTU!="" || $xeClnsMTU!="")
            interface $gv.service-l3Link-interfaceName
             #if($xeMTU!="")
                    no mtu $xeMTU
             #end
             #if($xeClnsMTU!="")
                    no clns mtu $xeClnsMTU
             #end
               exit
          #end

           #if($gv.service-l3Link-routingProtocolName=="BGP")
           #if($addressFamily !="" && $addressFamily=="vpnv4")
            router bgp $gv.service-l3Link-routerProcessId
             no address-family $addressFamily
               exit
           #end
           #end


 ##XR DEVICE
 #else
  #if($xrMTU!="")
   #if($gv.service-l3Link-subInterfaceName=="")
              interface $gv.service-l3Link-interfaceName
                  no mtu $xrMTU
                exit
```

```
            #end
        #end

        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily !="" && $addressFamily=="vpnv4")
         router bgp $gv.service-l3Link-routerProcessId
          address-family $addressFamily unicast
    no additional-paths receive
   exit
   neighbor $gv.service-l3Link-bgpNeighborName
           no address-family $addressFamily unicast
   exit
            exit

        #end
        #end

 #end

#end
```

Example Configuration 5: Extending a Bidirectional TE tunnel using a CLI template with a global variable and a template (local) variable:

```
##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
"MODIFY")
  #if($variant && $variant=="IOS-XE")
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
         #if($xeBandWidth && $xeBandWidth !="")
               interface Tunnel$gv.service-teTunnel-tunnelId
                  bandwidth $xeMaxBandWidth
                      tunnel mpls traffic-eng auto-bw frequency $xeBandWidth max-bw
$xeMaxBandWidth min-bw $xeMinBandWidth
               exit
          #end
   #end
 #else
      #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
     #if($xrBandWidth && $xrBandWidth!="")
             interface tunnel-te$gv.service-teTunnel-tunnelId
                 bandwidth $xrMaxBandWidth
                 auto-bw
                      bw-limit min $xrMinBandWidth max $xrMaxBandWidth
                     application $xrBandWidth
               exit
             exit
        #end
 #end
 #end
#elseif($gv.service-serviceOperationType == "DELETE")
 #if($variant && $variant=="IOS-XE")
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
  #if($xeBandWidth && $xeBandWidth!="")
              interface Tunnel$gv.service-teTunnel-tunnelId
                 no bandwidth
                 no tunnel mpls traffic-eng auto-bw
              exit
          #end
   #end
 #else
      #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
          #if($xrBandWidth && $xrBandWidth!="")
             interface tunnel-te$gv.service-teTunnel-tunnelId
                 no bandwidth
```

```
                no auto-bw
            exit
        #end
 #end
 #end

#end
```

Example Configuration: Rollback Template

You can create a rollback template and use it if the deployment fails. Navigate to Configuration > Templates > Features and Technologies, then choose CLI Templates to configure a custom rollback template. While configuring the template you must use #ROLLBACK_CONFIG_START and #ROLLBACK_CONFIG_END as flags for rollback. You must specify what the CLI needs to rollback to in between these flags. It can be used for both pre and post service configuration.

Note These rollback templates are not applicable for optical services.

Sample template format:

```
#ROLLBACK_CONFIG_START
interface GigabitEthernet0/0/20
mtu 1555
#ROLLBACK_CONFIG_END
```

Example Configuration 1: Rollback of preconfig CLI without parameters:

CLI example:

```
snmp-server enable traps
FAIL here
vrf definition PreConfigTest
 vpn id 12:566
 rd 23.23.23.23:2
 address-family ipv4
  route-target import 32:1
  route-target export 32:1
interface GigabitEthernet0/10
 service instance 3 ethernet
  encapsulation dot1q 521
  rewrite ingress tag pop 1 symmetric
  bridge-domain 8
 exit
interface Vlan8
 no shutdown
 mtu 1522
 vrf forwarding PreConfigTest
 ip address 33.44.24.55 255.255.255.0
router bgp 100
 address-family ipv4 vrf PreConfigTest
  exit
```

Example Configuration 2: RollBack of postconfig CLI without parameters:

CLI example:

```
snmp-server enable traps
vrf definition PreConfigTest
 vpn id 12:566
```

```
 rd 23.23.23.23:3
 address-family ipv4
  route-target import 24:1
  route-target export 24:1
interface GigabitEthernet0/10
 service instance 4 ethernet
  encapsulation dot1q 685
  rewrite ingress tag pop 1 symmetric
  bridge-domain 9
 exit
interface Vlan9
 no shutdown
 mtu 1522
 vrf forwarding PostConfigTest
 ip address 23.44.55.56 255.255.255.0
router bgp 100
 address-family ipv4 vrf PostConfigTest
  exit
 exit
snmp-server enable traps
FAIL here
```

Example Configuration 3: PreConfig working template, Post config invalid template, Deployment failure and rollback CLI

CLI example:

```
snmp-server enable traps
vrf definition PrePostConfig
 vpn id 34:55
 rd 23.23.23.23:4
 address-family ipv4
  route-target import 234:1
  route-target export 234:1
interface GigabitEthernet0/10
 service instance 5 ethernet
  encapsulation dot1q 664
  rewrite ingress tag pop 1 symmetric
  bridge-domain 11
 exit
interface Vlan11
 no shutdown
 mtu 1522
 vrf forwarding PrePostConfig
 ip address 44.55.22.55 255.255.255.0
router bgp 100
 address-family ipv4 vrf PrePostConfig
  exit
 exit
snmp-server enable traps
FAIL here
```

Example Configuration: Interactive Template

Example Configuration 1: Interactive template for commands that have single prompt:

Template Format:

```
#INTERACTIVE
no username test<IQ>confirm<R>y
#ENDS_INTERACTIVE
```

CLI example (Template set as Pre-service configuration):

```
no username test
bridge-domain 8
ethernet cfm domain EVC level 4
  service b_evplan_4Mar evc b_evplan_4Mar vlan 8
    continuity-check
    continuity-check interval 1s
ethernet evc b_evplan_4Mar
  oam protocol cfm domain EVC
interface GigabitEthernet0/0/1
  ethernet uni id UniName3
  service instance 2 ethernet b_evplan_4Mar
    encapsulation dot1q 22
    bridge-domain 8
    cfm mep domain EVC mpid 1
    ethernet lmi ce-vlan map 22
    snmp trap link-status
    exit
  exit
```

Example Configuration 2: Interactive template for commands that more than one prompt:

Template Format:

```
#INTERACTIVE
crypto key generate rsa<IQ>% Do you really want to replace them? [yes/no]:<EM><R>yes<IQ>How
 many bits in the modulus [512]:<EM><R>512
#ENDS_INTERACTIVE
```

CLI example (Template set as Post-service configuration):

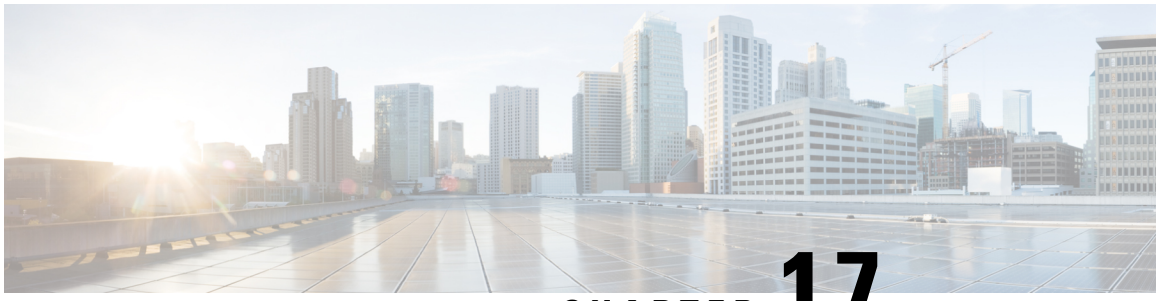
```
bridge-domain 8
ethernet cfm domain EVC level 4
  service b_evplan_4Mar evc b_evplan_4Mar vlan 8
    continuity-check
    continuity-check interval 1s
ethernet evc b_evplan_4Mar
  oam protocol cfm domain EVC
interface GigabitEthernet0/0/0
  ethernet uni id UniName4
  ethernet lmi interface
  service instance 1 ethernet b_evplan_4Mar
    encapsulation dot1q 345
    bridge-domain 8
    cfm mep domain EVC mpid 1
    ethernet lmi ce-vlan map 345
    snmp trap link-status
    exit
  exit
crypto key generate rsa
```

Provisioning failure syslog

When a service provisioning failures occurs, EPNM generates a syslog and sends it to the receivers that are configured in the EPNM. This syslog is generated for create, modify, delete, and promote operations.

The receiver can be configured by CLI by logging into the EPNM server. See Connect via CLI, on page 752. Execute **`logging security <syslog receiver ip>`** in **`conf`** mode.

The visual representation of the syslog depends on the software used on the receiver machine/server.



CHAPTER 17

View and Manage Discovered/Provisioned Circuits/VCs

Enable and Disable Service Discovery

Cisco EPN Manager uses the service discovery feature to automatically discover the circuits/VCs existing in the network and the circuits/VCs that are provisioned using the Provisioning Wizard.

The service discovery feature is enabled by default. You can choose to disable this feature. If you disable service discovery, all the discovered services in Cisco EPN Manager will be removed. However, the services that were provisioned using Cisco EPN Manager remain in 'Missing' state. Use the **History Settings** option to configure the maximum number of versions of a discovered Circuit/VC changes that are presented in the Circuit/VC History table. You must restart the server to apply the changes.

Note The **History Settings** configuration is relevant only for discovered changes in optical circuits.

To disable service discovery:

Step 1 From the left side bar, choose **Administration** > **Settings** > **System Settings**, then choose **Circuits/VCs** > **Discovery Settings**.

Step 2 Uncheck the **Enable Service Discovery** checkbox.

Step 3 Restart Cisco EPN Manager to apply your changes. See Stop and Restart Cisco EPN Manager, on page 769

Circuit or VC States

Circuit or VC Primary States—conveys the most important state information for a circuit, in this order: Serviceability, Discovery, Alarm, Provisioning. It is normally shown in the first column of a circuit or VC table.

Circuit or VC Primary State	Icon	Serviceability	Discovery	Alarm	Provisioning
Missing		—	Missing	—	—
Down		Down	—	—	—
Critical		—	—	Critical	—
Major		—	—	Major	—
Minor		—	—	Minor	—
Partially Down		Partial	—	—	—
Admin Down		Admin Down	—	—	—
Partially Discovered		—	Partial	—	—
Failed		—	—	—	(Create, modify, or delete) failed
In progress		—	—	—	(Create, modify, or delete) in progress
Warning			—	Warning	—
Up		Up	—	—	—

Circuit or VC Serviceability State—this value is a combination of the circuit or VC's admin and operational states. The admin state is shown because it impacts service operability. For optical circuits, the admin state also determines whether the Activate and Deactivate actions are available. The operational state is shown to quickly identify whether a service is working or not.

Circuit or VC Serviceability State	Icon	Description
Admin Down		Circuit or VC manually shutdown by the administrator.
Down		Circuit or VC is operationally down and administratively up.
Up		Circuit or VC is operationally and administratively up.
Auto Up		Circuit or VC is operationally auto up and administratively up. Only certain devices support the Auto Up operational state.
Unavailable		Circuit or VC has not been discovered yet, or its operational status is unavailable.
Partial		Circuit/VC operational or administrative state is partial. • Partial admin state—The circuit or VC has a mixed administrative request (to activate some service resources and deactivate others), has a mix of resources that are administratively up and down, or has resources whose operational state is unavailable. • Partial operational state—The circuit or VC has a mix of some active and deactivated resources, or the operational state for some of its resources are unavailable.
Up - Unprotected		The circuit/VC that was configured with a protection path is operational but cannot switch to the alternate path because of severe failures. **Note** This serviceability status indication is supported for OCHCC WSON circuits with Y-Cable protection and protected ODU.

Following table provides details of the serviceability states of Circuits/VCs under various scenarios:

Technology	Service Type	Scenario	Serviceability State

Carrier Ethernet	EPL, EVPL, Access EPL, and Access EVPL	If the operational state of the endpoints (service instance / subinterface), cross connects, and pseudowire participating in the service is up	Up
		If the admin state of both the source and destination endpoints (service instance / subinterface) participating in the service is down	Admin Down
		In all the other scenarios, when at least one endpoint (service instance / subinterface), cross connect, or the pseudowire participating in the service is down	Down
	EP-LAN, EVP-LAN, EP-Tree, and EVP-Tree	If all the endpoints (service instance / subinterface), bridge domains, VFIs, and pseudowires participating in the service are up	Up
		If the operational state of at least two endpoints (service instance / subinterface) participating in the service are up and the rest of the endpoints are down	Partial
		If the admin state of all the endpoints (service instance / subinterface) participating in the service is down	Admin Down
		If the operational state of at least one endpoint (service instance / subinterface) participating in the service is up and the rest of the endpoints are down	Down

Circuit Emulation	All service types	If the operational state of the endpoints (cemGroup), underlying TDM controller, cross connect, and pseudowire participating in the service are up	Up
		If the admin state of both the source and destination endpoints (cemGroup) participating in the service is down	Admin Down
		In all the other scenarios, when the operational state of one of the endpoints (cemGroup), underlying TDM controller, cross connect, and pseudowire participating in the service is down	Down
MPLS	Unidirectional TE Tunnel	If the operational state of the tunnel interface is up	Up
		If the admin state of the tunnel interface is down	Admin Down
		In all the other scenarios, when the operational state of the tunnel is down	Down
	Bidirectional TE Tunnel	If the operational states of the interfaces on both ends of the tunnel is up	Up
		If the admin states of the interfaces on both ends of the tunnel is down	Admin Down
		In all the other cases, when the operational state of the tunnel interface is down	Down

Serial	RS232, RS422, and RS485	If the operational state of the endpoints (channelGroup), underlying Serial interface, cross connect, and pseudowire participating in the service are up	Up
		If the admin state of both the source and destination endpoints (channelGroup) participating in the service is down If the admin state of either source or destination endpoint (channelGroup) is down	Admin Down
		In all the other scenarios, when the operational state of one of the endpoints (channelGoup), underlying Serial interface, cross connect, and pseudowire participating in the service is down	Down
	Raw Socket	If server and all its associated client sessions are up	Up
		If server is up and all its associated client sessions are down	Down
		If the admin state of both the source and destination endpoints (channelGroup) participating in the service is down If the admin state of a server or admin state of all the participating clients are down	Admin Down
		If server and all its associated client sessions are down	Down

		If server is up and if any one of its associated clients is up	Partial
Layer 3 VPN		If the operational state of all the endpoints (subinterface, BDI, and BVI) participating in the service is up	Up
		If the operational state of at least two endpoints (subinterface, BDI, and BVI) participating in the service are up and the rest of the endpoints are down	Partial
		If the admin state of all the endpoints (subinterface, BDI, and BVI) participating in the service is down	Admin Down
		If the operational state of at least one endpoint (subinterface, BDI, and BVI) participating in the service is up and the rest of the endpoints are down.	Down
SR TE	SR Policy	If the operational state of the SR policy us up	Up
		If the admin state of the SR policy is down	Admin Down
		In all the other scenarios, if the operational state of the SR policy is down	Down

Circuit or VC Discovery State—Represents the latest state and structure of a service and its components, as discovered from the network. Having a Discovered version means that the application is actually monitoring the service itself, for example, it can define meaningful operational and performance data.

Pseudowire Serviceability State—The icons next to the **Link Name** represents the state that the pseudowire is in. The  arrow represents that the link is up while the  arrow represents it is down.

Circuit or VC Discovery State	Icon	Description
Partial		Circuit or VC partially discovered by Cisco EPN Manager; not all its expected entities have been discovered.

Full		Circuit or VC fully discovered by Cisco EPN Manager, so Cisco EPN Manager can monitor the service and provide meaningful operational and performance data.
Missing		Circuit or VC not yet discovered by Cisco EPN Manager (though it may have been provisioned).
Resync		Circuit or VC is resynced.

Circuit or VC Provisioning State—Represents whether there is a provisioning intent for a circuit or VC and, if so, its status. If a reconciliation report has been generated, the state of the reconcile action is reflected.

Circuit or VC Provisioning State	Icon	Description
None		Circuit or VC was discovered but has not yet been provisioned. The circuit/VC must be promoted in order to modify or delete it.
Failed		Action has failed.
In Progress		Action was initiated but not yet completed.
Planned		Action is planned but not yet initiated.
Succeeded		Action has completed successfully.

View Circuits/VCs

Cisco EPN Manager provides a variety of ways that you can view circuits/VCs:

To view circuit/VC information for:	See the procedures in:
A specific circuit/VC in a topology map, in a Circuit/VC 360 view, or in a Circuit/VC Details page	• Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 629 • Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window, on page 635
A device	View a Specific Device's Circuits/VCs, on page 637
A device group in a topology map or in an expanded table	View a Device Group's Circuits/VCs, on page 638
All of Cisco EPN Manager	View All Circuits/VCs in Cisco EPN Manager, on page 639

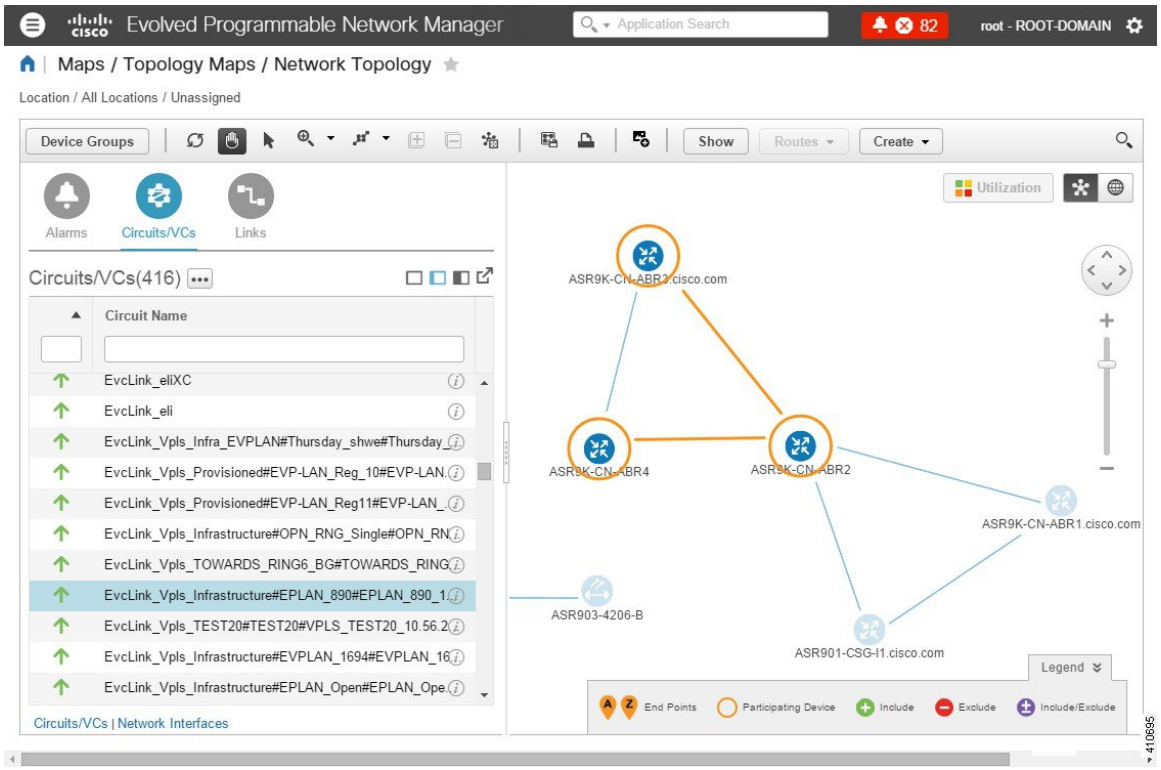
View a Specific Circuit/VC's Details

Cisco EPN Manager provides different ways to view details about a specific circuit/VC, depending on how much detail you need:

View a Specific Circuit/VC in the Topology Map

When working with circuits/VCs, it is very useful to see how a circuit/VC is deployed within the existing network topology. Cisco EPN Manager overlays the circuit/VC on an existing topology map, clearly indicating the endpoints and midpoints of the circuit/VC, the role of the endpoint (where relevant), and relevant fault information for the circuit/VC. This overlay functionality is available in the geo map as well as the topology map.

For CE and CEM services that use the MPLS TE tunnels to traverse through the network, the underlying tunnel is also displayed in the topology map along with the service overlay. For information about how to assign a MPLS TE tunnel for a CE or CEM service, see Provision EVCs in a Carrier Ethernet Network, on page 507 and Provision Circuit Emulation Services, on page 573 .



Note

- The overlay cannot be displayed if the discovery state of the circuit is "Missing".
- A circuit/VC might contain endpoints that cross device groups, meaning that one endpoint might belong to one group and another might belong to a different group. In this case, the full overlay cannot be shown. If an endpoint is not currently shown in the map, a notification link will appear at the top left of the map. Click the link to expand the map to show all the device groups that contain endpoints of the selected circuit/VC.
- When the overlay is displayed, the Link Type filter is disabled.

To display an overlay of a circuit/VC on the network topology:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Device Groups** button and select the required group.

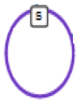
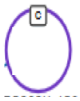
Step 3 Go to the Circuits/VCs tab to see a list of the circuits/VCs associated with the selected group.

Step 4 Select the circuit/VC you want to see on the map.

The nodes and links that participate in the selected circuit are highlighted in the overlay and the rest of the devices in the map appear disabled. The name of the selected circuit is displayed just below the topology toolbar. To clear the overlay, click the 'x' button to the right of the circuit name. For a description of the overlay icons, see Circuit or VC Network Topology Overlay Icons.

Circuit or VC Network Topology Overlay Icons

Overlay Icon	Definition
	Source endpoint
	Destination endpoint
	EVC or CEM service with local switching
	Endpoint included by the user during creation o **Note** "S" appears for both adjacent and n
	Endpoint excluded by the user during the creatio

Overlay Icon	Definition
	Endpoint with some ports that were either in routes of the circuit.
	E-TREE EVC endpoint that has been design
	S on the icon represents that the server is co
	C on the icon represents that the client is co
	S and C on the icon represents that both serv
	Selected endpoint.
	Hub; If the hub and root are on the same dev
	Link included during creation of the circuit.
	Link excluded during creation of the circuit.
	Endpoint with some ports that were either in participating in various routes of the same ci

Get Quick Information About a Circuit/VC: Circuit/VC 360 View

The Circuit/VC 360 view provides at-a-glance information about a specific circuit/VC. From the Circuit/VC 360 view, you can access detailed information about the circuit/VC and perform the actions described in Actions You Can Perform from the Circuit/VC 360 View, on page 633.

The Circuit/VC 360 view displays the circuit name, state, and general circuit/VC and performance information at the top of the view. More detailed information is provided in tabs in the lower part of the view.

Information Provided in Circuit/VC 360 View	Description
General information	Type of circuit/VC, its various states (discovery, serviceability, provisioning), the customer associated with the circuit/VC, and some audit information (when it was created, when it was last changed). For an explanation of circuit/VC states, see Circuit or VC States, on page 620. **Note** If the Provisioning state is **Create Failed**, click the associated *i* (**information**) icon to see the reason for the failure. Auto-Refresh— For real-time updates of status and troubleshooting, enable an on-demand refresh by clicking on the Refresh icon. Alternatively, you can also set the auto-refresh interval to 30 seconds, 1 minute, 2 minutes or 5 minutes from the drop-down list. Auto-Refresh is OFF by default. **Note** The Auto-Refresh setting is applicable only for the currently open 360 view popup window. If the view is closed and reopened or another view is opened, by default Auto-Refresh is Off. The reserved bandwidth utilization of the TE tunnel is displayed based on the bandwidth configured on the tunnel compared to the bandwidth configured on the Pseudowire associated to the tunnel.
Performance data	Graphs reflecting various aspects of the circuit/VC performance. **Note** For data to be shown in the graphs, the required monitoring policy must be activated for the relevant devices. For example, to view graphs that chart the number of Explicit Pointer Adjustment Relay counters (such L-bits and P-bits) that have been generated and received, both the CEM and Pseudowire Emulation Edge to Edge monitoring policies must be enabled. See Monitoring Policies Reference, on page 949.
Alarms	Current alarms for the circuit/VC, including their severity, status, and the time they were generated.
Endpoints	Devices and interfaces that serve as endpoints for this circuit/VC.
EVIs	This tab displays the EVI endpoints. The **EVI Details** tab displays the EVI details, route targets, and route policies configured for the selected endpoints.

History	The **History** tab lists all versions of the circuit, allowing you to view the changes that have occurred since the circuit/VC was discovered or first deployed. You can open the Circuit 360 view for any of the versions listed to see its endpoints, alarms, and so forth. **Note** If you are looking at the Circuit 360 view for a historical circuit/VC, the **History** tab is not displayed. You can also view the configuration details for the circuit/VC's endpoints by doing the following: **1.** Locate the appropriate circuit/VC version and click its *i* (**information**) icon in the **Provisioning State** column. The **Device Configuration Details** pop-up window opens. **2.** Click the radio button for the endpoint whose configuration details you want to view. If the endpoint was successfully provisioned, its configuration is listed at the bottom of the pop-up window. If provisioning of the endpoint failed, a description of why provisioning failed is listed instead.
Related Circuits/VCs	Additional circuits within the selected circuit.

For EVCs, the following information is shown:

- Incoming Traffic—The sum of incoming traffic, in bits per second (bps), entering all the endpoint interfaces of the circuit/VC over time. The graph shows the last 24 samples of the total incoming traffic for all the endpoints in intervals of 1 minute. The pink bar shows the lowest level of incoming traffic while the blue bar shows the highest level of incoming traffic.
- Port Availability—Average availability of all the endpoints of the circuit/VC, expressed as a percentage, aggregated across all endpoints. Baseline is 100% unless any of the interfaces has been unavailable.
- Outgoing Traffic—The sum of traffic, in bits per second (bps), exiting all the endpoint interfaces of the circuit/VC over time.
- Loss—Average loss, expressed as a percentage, across all the endpoints of the circuit/VC.
- Delay—Average delay, in microseconds, across all the endpoints of the circuit/VC.
- Jitter—Average jitter, in milliseconds, across all the endpoints of the circuit/VC.

For optical circuits, the performance data is shown based on the following circuit types:

- OCHCC WSON—The total number of octets received on the interface, including frames, number of inbound packets with errors that prevented them from being delivered to a higher layer protocol, and number of severely errored seconds per line and multiplex sections.
- OCHNC WSON—The average, minimum, maximum optical signal to noise ratio (OSNR), and electrical signal to noise ratio (eSNR) for this circuit type.
- OCH-TRAIL WSON—The total number of uncorrectable words and the total number of errors corrected, in bits per second (bps), for this circuit type.

- OCH-Trail UNI—The total number of uncorrectable words and the total number of errors corrected, in bits per second (bps), and the minimum, average, and maximum output power received and transmitted, in decibel referenced to 1 watt (dBW) by this circuit type.
- ODU UNI—The total number of background block errors, total number of severely errored seconds, and errored seconds ratio for path monitoring.
- ODU Tunnel—The total number of background block errors, total number of severely errored seconds, and errored seconds ratio for section monitoring.

In addition, the average, minimum, and maximum amount of output power received and transmitted from the circuit is shown for all optical circuit types.

For Circuit Emulation services, the following information is shown:

- The total number of jitter buffer overruns for each circuit endpoint.
- The total number of Explicit Pointer Adjustment Relay counters (such as L-bits and R-bits) that were generated and received for each circuit endpoint.

For services on a Cisco ME 1200 device, information such as incoming and outgoing traffic, jitter, and availability is displayed.

For MPLS bidirectional TE tunnels, ensure that you activate the Interface Health monitoring policy so that the performance data is shown. See Monitoring Policies Reference, on page 949 for more information. The following performance data is shown:

- Traffic—The sum of traffic in both directions of the tunnel, in bits per second (bps).
- Availability—Average availability of the endpoints in the tunnel.
- Bandwidth Utilization—The percentage of bandwidth configured on the tunnel against the sum of the percentage of bandwidth configured on all the pseudowires associated with the tunnel.
- Actual Bandwidth Utilization—The percentage of bandwidth configured on the tunnel against the sum of the percentage of bandwidth utilized for the incoming and outgoing traffic in all the pseudowires associated with the tunnel.

For Carrier Ethernet services that have Y.1731 probes enabled, view the extended details of Y.1731 probes in the **Y.1731** tab.

Note In the **Endpoints** tab, choose a relevant endpoint and then click the *i* icon to view the extended details.

To open the **Circuit/VC 360** view for a particular circuit or VC:

Step 1 Choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens. See Visualize the Network Topology, on page 173 for a description of the network topology window and its functionality.

Step 2 From the **Network Topology** page toolbar, click **Device Groups**.

The **Device Groups** dialog box opens.

Step 3 Locate and click the device group that the circuit or VC is associated with, then close the dialog box.

Step 4 Click the **Circuits/VCs** tab.

Step 5 Locate the circuit or VC in the list and then click its *i* (**information**) icon.

Actions You Can Perform from the Circuit/VC 360 View

The following is a list of the actions you can perform from the **View** and **Actions** menus for the selected circuit or VC. The actions that are available will vary, depending on the type of circuit or VC that is selected:

- Choose **View > Details** to display further details about the circuit/VC. See Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window, on page 635.

Note The **View > Details** is not supported for the IOT services (RS232, RS422, RS485, Raw Socket, C37.94, EM-Voice, and X.21 service details).

- Choose **View > Service Trace** to trace the route of an optical circuit. See Trace and Visualize the Full Route of a Circuit, on page 197 .
- Choose **View > Dashboard** to view the service performance dashboard of the circuit/VC. See Set Up and Use the Dashboards, on page 4.
- Choose **View > Performance** to view the circuit details and the CEM statistics of the CEM services.
- Choose **Actions > Add to Compare** to select the circuit or VC for a side-by-side comparison with another circuit or VC on the basis of information such as serviceability and provisioning state and raised alarms. See Compare Circuit/VC Information and Status.
- Choose **View > Multilayer Trace** to visualize a circuit in a graphical manner. See Trace and Visualize the Full Route of Circuits/VCs.
- Choose **Actions > Y.1564 Test** to test the performance of the CE circuit/VC end to end. See Running a Y.1564 Performance Test, on page 668.
- Choose **Actions > Y.1731 Test** to test the performance of the CE circuit/VC end to end. See Performance Test Based on Y1731 for EVCs, on page 670.
- Choose **Actions > BERT** to test the performance of the Circuit Emulation Services. See Performance Test for Circuit Emulation Services, on page 673.
- Choose **Actions > Optical PM Parameters** to view the real time performance monitoring data of the optical circuit/VC. See Optical Performance Monitoring Parameters, on page 671.
- Choose **Actions > PRBS Test** to test the performance of the optical circuit/VC end to end. See Run PRBS Test on Circuits (ODU UNI), on page 672.
- Choose **Actions > Restoration Actions >Upgrade Restore** to upgrade the failed optical circuit to an active route and delete the old route where the failure occurred. See Restore a Circuit (Optical), on page 645.
- Choose **Actions > Restoration Actions >Manual Revert** to revert the optical circuit to its original route when the route has recovered from the failure. See Revert a Circuit (Optical), on page 646.
- Choose **Actions** > **Maintenance Actions** > **Repair** to repair the failed optical circuit on the same path where the failure has occurred. See Repair a Circuit (Optical), on page 647.

- Choose **Actions** > **Reroute Actions** > **Working Path** or **Protected Path** to reroute the traffic through the working path or protected path defined for the circuit. See Reroute a Circuit (Optical), on page 646.
- Choose **Actions > Activate** to allow the traffic to pass through the optical circuit. See Activate a Circuit (Optical), on page 644.
- Choose **Actions > Deactivate** to stop the traffic passing through the optical circuit. See Activate a Circuit (Optical), on page 644.
- Choose **Actions > Pseodowire OAM** or **LSP OAM** or **CFM OAM** or **SR TE OAM** option to troubleshoot a service failure using OAM commands. See Troubleshoot a Service Failure Using OAM Commands, on page 662.
- Choose **Actions** > **Show in Topology** to view the circuit/VC overlay in the topology map.
- Click the *i* icon next to the Serviceability status to view additional information about a circuit failure. See Get More Information About a Circuit/VC Failure, on page 661.
- Choose **Actions** > **Resync** > to perform the service discovery resync pertaining to a particular service. For more information, see Service Discovery Resync.

Compare Circuit/VC Information and Status

From the **Comparison View**, you can perform a side-by-side comparison of multiple circuits or VCs, viewing information such as discovery and provisioning state, raised alarms, and associated endpoints. To compare circuits or VCs, do the following:

Step 1 For each circuit or VC you want to compare:

a) Open its **Circuit/VC 360** view, as described in Get Quick Information About a Circuit/VC: Circuit/VC 360 View.

b) Choose **Actions** > **Add to Compare**.

The circuit or VC you selected is displayed at the bottom of the page. You can select a maximum of 4 circuits and VCs.

Step 2 Click **Compare**.

The **Comparison View** opens.

Step 3 From the drop-down list at the top of the view, specify whether the view will show all available information or just the information that is unique to each device.

Step 4 Click **Comparison View**, check the check box for the categories you want the view to display, and then click **Save**.

By default, all of the categories are already selected.

Step 5 Scroll down the page to view the information provided for each category you selected.

Note the following:

- The **Comparison View** only displays information for two circuits or VCs at a time. If you selected more than two, you will need to toggle to the circuits or VCs that are not currently displayed.
- To reorder the circuits or VCs you have selected, click **Rearrange**.
- Each circuit or VC's **View** and **Actions** menu is identical to the ones provided in its **Circuit/VC 360** view. If you select an option, the corresponding page opens.

- You can minimize and maximize the categories displayed, as needed.
- The **Comparison View** is also available for devices, interfaces, and links. Whenever you select any of these elements from their respective 360 view for comparison, they are displayed in the corresponding tab. This allows you to switch between element types, as needed.
- When you are done comparing circuits or VCs, click **Back** at the top of the view and then click **Clear All Items** at bottom of the page. If tabs for other element types are still displayed, you will need to clear them as well.

Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window

The Circuit/VC Details window provides additional details about a specific circuit/VC, including the attributes defined for the circuit/VC. The information shown in the displayed page varies depending on the type of circuit/VC. You can also perform certain actions from the Circuit/VC Details Window, for example, modify/delete the circuit/VC, create a new circuit/VC, run a performance test.

To access the Circuit/VC Details window, click on the circuit/VC name hyperlink in any of the circuit/VC tables. Alternatively, you can access the Circuit/VC details window from the Circuit/VC 360 view, as follows:

Step 1 Access the Circuit/VC 360 view for the required circuit/VC. See Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 629.

Step 2 Choose **View > Details**. See Provision EVCs in a Carrier Ethernet Network, on page 507 and Provision Circuits in an Optical/DWDM Network, on page 526 for description of the attributes in the Circuit/VC details page.

The details are displayed in two tabs:

- **Summary**: Displays circuit information such as the circuit discovery and provisioning states, acceptance threshold, WSON label, circuit type, wavelength associated with the circuit, protection status, and more.
- **Ports**: Displays ports information such as the ports associated with the circuit, their port roles, the IP addresses associated with the ports, and more

Actions You Can Perform from the Circuit/VC Details Page

From the Circuit/VC Details window, you can do the following:

- Modify the circuit/VC (action available for circuits/VCs provisioned using Cisco EPN Manager). See Modify a Circuit/VC, on page 644.
- Delete the circuit/VC (action available for circuits/VCs provisioned using Cisco EPN Manager, not for discovered circuits/VCs). See Delete a Circuit/VC, on page 651.
- Create a new circuit/VC. Clicking the Create button opens the Provisioning Wizard, enabling you to create a new circuit/VC. See Provision EVCs in a Carrier Ethernet Network, on page 507 and Provision Circuits in an Optical/DWDM Network, on page 526.
- Choose **Actions > Y.1564 Test** to test the performance of the CE circuit/VC end to end. See Running a Y.1564 Performance Test, on page 668.

- Choose **Actions > BERT** to test the performance of the Circuit Emulation Services. See Performance Test for Circuit Emulation Services, on page 673.
- Choose **Actions > Optical PM Parameters** to view the realtime performance monitoring data of the optical circuit/VC. See Optical Performance Monitoring Parameters, on page 671.
- Choose **Actions > PRBS Test** to test the performance of the optical circuit/VC end to end. See Run PRBS Test on Circuits (ODU UNI), on page 672.
- Choose **Actions > Restoration Actions >Upgrade Restore** to upgrade the failed optical circuit to an active route and delete the old route where the failure occurred. See Restore a Circuit (Optical), on page 645.
- Choose **Actions > Restoration Actions >Manual Revert** to revert the optical circuit to its original route when the route has recovered from the failure. See Revert a Circuit (Optical), on page 646.
- Choose **Actions** > **Maintenance Actions** > **Repair** to repair the failed optical circuit on the same path where the failure has occurred. See Repair a Circuit (Optical), on page 647.
- Choose **Actions > Activate** to allow the traffic to pass through the optical circuit. See Activate a Circuit (Optical), on page 644.
- Choose **Actions > Deactivate** to stop the traffic passing through the optical circuit. See Activate a Circuit (Optical), on page 644.
- Choose **Actions > Resync** to resynchronize circuit. See Resynchronize a Circuit/VC, on page 650.

View and Compare Versions of a Circuit (Optical)

Use the Circuit History page to compare two versions of an optical circuit. From the Circuit History page, you can:

- Get a simple visualization and integrated view of the events that occurred in an optical circuit.
- View the alarms associated with an event.
- View information about a failure that occurred in an optical circuit.
- Compare the route changes in a circuit.

For example, consider that there is a restoration that has occurred in an optical circuit. Using the Circuit History page, you can:

1. View the list of changes that had occurred in the circuit.
2. If there is a protection switch action or a reroute that had occurred in the circuit, you can click the *i* icon in the Type column to see the details of the event that has caused the protection switch action or the reason for the failure occurred because of the reroute action.
3. Click the *i* icon in the Time Stamp column to see the alarms that are associated with the event.
4. You can further compare the route changes between the active path and the path at the time of protection switch.
5. You can also choose to compare the route changes between the active path and the original path or between the original path and the path at the time of protection switch to view the difference in the participating nodes and take action on the affected nodes.

To view the history of an optical circuit:

Step 1 From the left side bar, choose **Maps** > **Topology Maps** > **Network Topology.**

Step 2 Click **Device Groups**, and then select the location in which the required circuit/VC was created.

Note By default, **All Location** group is selected.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

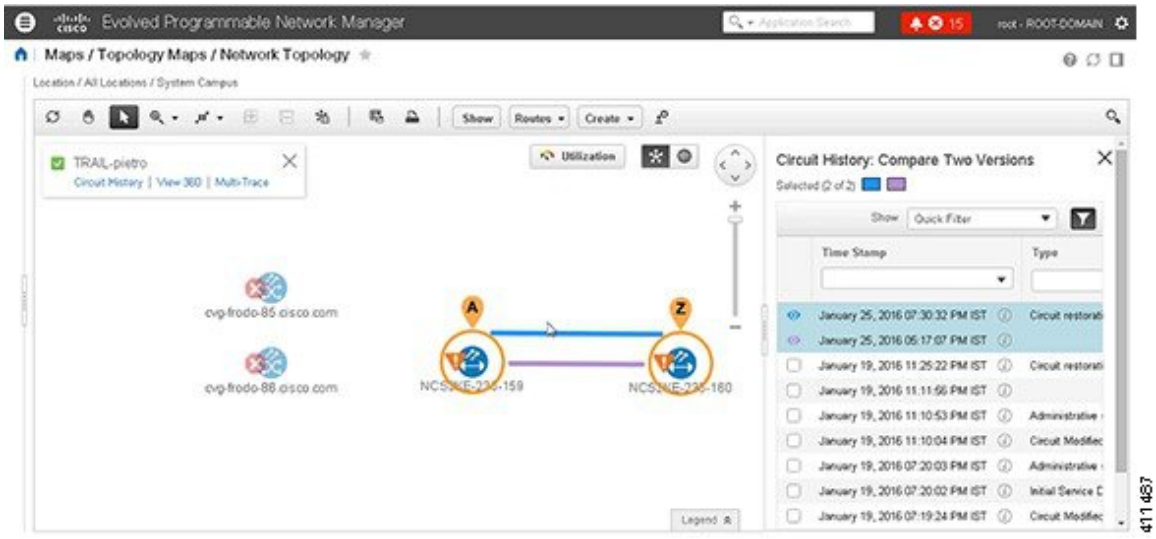
Step 5 Select the optical circuit for which you want to view the history. The overlay of the circuit is displayed on the map.

Step 6 Click the **Circuit History** hyperlink that appears right below the topology toolbar.

The **Circuit History** area is displayed next to the topology map and lists the various versions of the circuit. The active route of the circuit is selected by default and it is displayed on the map.

Step 7 Select a history version from the list displayed in the **Circuit History** area to compare it with the current version.

The overlay on the map changes based on your selection and displays both, the active route and the history version. You can select and compare only two versions at a time.



View a Specific Device's Circuits/VCs

Use the Device 360 view to see a list of all the circuits/VCs in which a specific device participates. This is useful when a specific device is having a problem and you want to see which services it will affect.

To view a list of circuits/VCs in which a device participates:

Step 1 Click the required device in the network topology (**Maps** > **Topology Maps** > **Network Topology**).

Step 2 Click **View 360** in the popup window.

Step 3 Go to the Circuit/VC tab in the Device 360 view to see a table listing the relevant circuits for that device. The table lists the circuit/VC name, the circuit/VC type, when it was created/modified, and the current status of the circuit/VC.

View a Device Group's Circuits/VCs

View a Device Group's Circuits/VCs List in the Topology Window

Cisco EPN Manager displays discovered and provisioned circuits/VCs in the Circuits/VCs tab on the left side of the network topology window. The list of circuits/VCs is filtered according to the selected device group. You can get details about the circuit/VC by clicking on the circuit/VC name to launch the Circuit/VC Details window or by clicking the information icon and launching the Circuit/VC 360 view.

The Circuits/VCs tab lists discovered circuits/VCs and the latest version of circuits/VCs provisioned using Cisco EPN Manager. The circuits/VCs are sorted by primary state (default).

To view a list of circuits/VCs in the network topology window:

Step 1 Choose **Maps** > **Topology Maps** > **Network Topology** in the left navigation pane. The network topology window opens.

Step 2 Click the **Device Groups** button and select the group of devices you want to show on the topology map.

Step 3 Go to the Circuits/VCs tab to see a list of circuits/VCs relevant to the selected device group.

Step 4 Select a circuit/VC to view an overlay of the circuit/VC in the network topology, meaning that the circuit/VC endpoints and path are shown on top of the physical topology. Click on the circuit name hyperlink to see circuit details or click on the information icon next to the circuit/VC name to open the Circuit/VC 360 view.

Step 5 To open a tabular view of the circuits/VCs in a separate window, click **Circuit/VCs** below the list of circuits/VCs.

View a Device Group's Circuits/VCs in an Expanded Table

From the network topology window, you can open a table of circuits/VCs associated with the selected device group in a separate browser window. The table provides more information about each circuit/VC and is also sortable and searchable, enabling you to find information easily. This table is particularly useful for identifying the provisioning status of circuits/VCs, as well as their management status within Cisco EPN Manager. For an explanation of circuit/VC states (and their icons, see Circuit or VC States, on page 620).

By default, the circuits/VCs table sorts the circuits/VCs by primary state. You can change how the table is sorted as required.

The expanded circuits/VCs table works together with the Network Topology window so that if you select a circuit/VC in the table, the circuit/VC will be represented graphically in the Network Topology window in the context of the topology map.

To open an expanded and more detailed tabular list of circuits in a separate window:

Step 1 Choose **Maps** > **Topology Maps** > **Network Topology** in the left navigation pane. The network topology window opens.

Step 2 Click the **Device Groups** button and select the group of devices you want to show on the topology map.

Step 3 Go to the Circuits/VCs tab to see a list of circuits/VCs relevant to the selected device group.

Step 4 Click the **Circuit/VCs** hyperlink below the list of circuits/VCs to open a separate window containing a list of circuits/VCs relevant to the selected device group.

- See more information about the circuit/VC by displaying the Circuit/VC 360 view. See View Circuits/VCs, on page 626.
- View the circuit/VC on the map, as an overlay on top of the displayed devices. See View a Specific Circuit/VC in the Topology Map, on page 627.
- Launch the Provisioning Wizard to provision circuits/VCs. See Create and Provision a New Carrier Ethernet EVC, on page 508 and Provision Circuits in an Optical/DWDM Network, on page 526.
- See more information about a circuit failure. See Get More Information About a Circuit/VC Failure, on page 661.
- Select a circuit/VC for modification, deletion, circuit trace, and performance test. See the following topics for more information:
  - Modify a Circuit/VC, on page 644
  - Delete a Circuit/VC, on page 651
  - Run a Performance Test on a Circuit/VC, on page 667

View All Circuits/VCs in Cisco EPN Manager

The **Circuits/VCs & Network Interfaces** page lists all of the circuits and VCs that Cisco EPN Manager is currently managing. From here, you can quickly locate a specific circuit or VC by filtering the list using basic criteria such as name, type, or customer. You can view the number of EFPs that Cisco EPN Manager has provisioned. If all the EFPs are provisioned, the number of EFPs will match the number of services. You can identify all of the circuits and VCs that have severe alarms or are in a specific state. (For a description of circuit and VC states (including primary states), see Circuit or VC States, on page 620.) You can also perform circuit and VC management tasks and run performance tests. To use this page, do the following:

Note After a device that is participating in a circuit or VC is removed from Cisco EPN Manager, the corresponding circuit or VC is still listed on the **Circuits/VCs & Network Interfaces** page.

Step 1 Choose **Inventory** > **Other** > **Circuits/VCs & Network Interfaces.**

Step 2 Perform any of the following actions:

- Find specific circuits or VCs by using one of the quick filter fields. For example, enter **L3VPN** in the **Type** field to list all circuits and VCs of that type or click the **Serviceability** quick filter field and then choose **Down** to view all circuits and VCs that are currently down.
- View a specific circuit or VC in the topology map by clicking its radio button and then choosing **Actions** > **Show in Topology**.
- With a circuit or VC selected, use the **Actions** menu to activate circuits or VCs and run performance tests.

- Create, modify, delete, or force delete circuits and VCs by clicking the appropriate button in the **Circuits/VCs & Network Interfaces** page toolbar, which opens the provisioning wizard.

Identify and Manage Discovered Circuits/VCs

Cisco EPN Manager discovers existing network circuits/VCs and displays them in the Circuit/VC list. Discovered circuits/VCs are automatically named by the system. The names for EVCs begin with **EvcLink_** (for example, EvcLink_Vpls_Bridge_318#318#VFIVPLS2_541549_10.56.23.48#1).

Note When circuits/VCs are discovered, the system identifies whether they are optical, CE, or L3VPN circuits/VCs, but it cannot identify the exact *type* of CE circuit/VC. For example, CE circuits/VC will display **EVC** in the Type column but not the type of EVC, such as EPL, E-LAN, and so on. For optical, the exact *type* of circuit is displayed.

You can do the following with discovered circuits/VCs:

- Identify discovered circuits/VCs in the Circuit/VC list by name or in the table of circuits/VCs by state, **Discovered**.
- View details about the discovered circuits/VCs in the Circuit/VC 360 view, including the endpoints of the circuit/VC.
- View an overlay of the circuit/VC on the network topology.
- View fault information for the circuit/VC.
- Promote a discovered circuit/VC, after which you can edit or delete it (applies to optical circuits and selected EVCs. See Promote a Discovered Circuit/VC Before Modifying/Deleting, on page 642.
- Do a performance test.

Show/Hide Implicit Circuits

A circuit is classified as implicit if it is an underlying or "carrying" circuit of another circuit. For example, an OCHTRAIL circuit could be a carrying circuit (and implicit) for an OCHCC circuit. By default, all circuits are listed in the circuit lists. However, you can hide implicit circuits from the lists, if required. When implicit circuits are hidden, they will not be displayed in the circuit lists but you can see them in the Carrying Circuits tab of the Circuit 360 view.

To hide implicit circuits from the circuit lists:

Step 1 From the left sidebar, choose **Administration > Settings > System Settings**.

Step 2 From the System Settings menu, choose **Circuits/VCs > Circuits/VCs Display**.

Step 3 Uncheck the Show Implicit Circuits/VCs check box.

Filter and Export the Circuit/VC list Based on a User Defined Field

You can create a user defined field, assign a value to the field, and associate it to a circuit/VC. You can then sort, filter, and export the circuit/VC list based on the user defined field.

For example, if you want to filter the circuit/VC list based on the service impact, you need to:

- Create a user defined field, named Service Impact
- Select the circuit/VC to which you want to associate the user defined field, Service Impact
- Assign the value as Critical, Moderate, or Low for the Service Impact field
- Sort, filter, and export the circuit/VC list based on the service impact value

Note You can create a maximum of 10 user defined fields.

Step 1 To create a user defined field, do one of the following:

- Choose **Administration** > **Settings** > **System Settings** > **General** > **User Defined Fields**, and then click the '+' icon to create a new label and description. Click **Save**.

  Note You cannot assign a value to the user defined field from the **Administration** menu.

- Choose **Inventory** > **Other** > **Circuits/VCs & Network Interfaces**, select a circuit/VC, and then choose **Actions** > **Manage User Defined Fields** . Click the '+' icon to create a user defined field, its description, and value. Click **Save**.
- Choose **Maps** > **Topology Maps** > **Network Topology**, go to the **Circuits/VCs** tab, and then click the Circuits/VCs hyperlink below the list of circuits/VCs. An expanded table of circuits/VCs opens in a separate window. Select a circuit/VC, and then choose **Actions** > **Manage User Defined Fields** . Click the '+' icon to create a user defined field, its description, and value. Click **Save**.

Step 2 In the Circuits/VCs & Network Interfaces page or in the expanded table of circuits/VCs, click the settings icon at the top right of the page, and then choose **Columns**.

Step 3 Choose the user defined field you have created, and then click **Close**. The user defined field with the assigned value is displayed as a column in the table of circuits/VCs.

Step 4 Click the Export icon next to the Settings icon at the top right of the table to export the data from the table to a file (CSV format).

You can delete the user defined field only from **Administration** > **Settings** > **System Settings** > **General** > **User Defined Fields**.

Display the Routes Associated With a Circuit

Use the network topology **Routes** drop-down menu to display specific routes associated for a circuit in the circuit overlay. Cisco EPN Manager calculates the routes from the links within a service. You can also filter the overlay based on the selected routes.

Note This feature is supported only on point-to-point CE services, optical circuits, and CEM services.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 From Device Groups list, select the required group. Cisco EPN Manager lists the circuits associated with the selected group in the Circuit/VCs tab.

Step 3 Click **Circuit/VCs**, and then select the circuit you want to display.

Step 4 From the **Routes** drop-down list, choose the required route type.

Note The route types are based on the routes configured on the selected circuit.

Promote a Discovered Circuit/VC Before Modifying/Deleting

Discovered circuits need to be promoted before they can be modified or deleted. After being promoted, the circuit/VC's provisioning state changes to Promote Successful.

Note Promotion is supported for Optical circuits, MPLS-TE, SR-TE and for basic EVCs that do not have additional configurations, such as LMI, QoS, G.8032, ICCP-SM. Promotion is supported if the underlying core is VPLS (for E-LAN and E-Tree EVCs). If a discovered circuit/VC cannot be promoted, it cannot be modified or deleted. Also, promotion is supported for Circuit Emulation' services, Unidirectional, Bidirectional, and L3VPN services.

Promotion of the CE services with CFM parameters such as CFM Domain name, CFM Domain level, Maint. Assoc. Name Type, ITU Carrier Code, ITU MEG ID Code, Continuity check interval, and IPSLA probes is supported. ITU Carrier Code and ITU MEG ID code will appear if ITU is selected in the Maint. Assoc. Name Type drop down list. Promotion of custom profile name for IPSLA probes in XR devices is not supported. The services will get promoted using custom profile name, but will not be listed during modification of the service.

Promotion of ICC-based CFM configuration on IOS XE and IOS XR devices is supported, except for the ME1200 devices. ICC based CFM is not supported for EVPN VPWS. EVPN based E-LAN service are not supported for promotion.

To promote a discovered circuit/VC:

Before you begin

For successful promotion of L3VPN services, ensure that the route distinguisher for the L3VPN service is specified in the format **rd device_ip:number**.

For example:

```
vrf definition vdvvgfr420
  rd 10.104.120.133:420
  vpn id 36B:420
  !
address-family...
```

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**. The network topology window opens.

Step 2 Click the **Device Groups** button and select the required group.

Step 3 Go to the Circuits/VCs tab and click the **Circuits/VCs** link to open an extended table of circuits/VCs in the selected group.

Step 4 Select the discovered circuit/VC you want to promote.

To identify L3VPN services that are discovered from the device but not promoted, filter out L3VPN services that have the provisioning status 'None'. You can also identify discovered services using the Name field of the L3VPN service. The Name field for L3VPN services that are discovered are represented with the service's unique VLAN IDs.

To identify MPLS TE services that are discovered from the device but not promoted, filter out MPLS TE services that have the provisioning status 'None'. You can also identify discovered services using the Name field of the MPLS TE service.

Step 5 Click **Modify**. The Provisioning Wizard opens.

Step 6 For optical circuits, modify the circuit as required, then click **Create**.

Step 7 For EVCs, do the following:

a) In the Endpoints Details page, select an endpoint. Fields relevant to the selected endpoint are displayed below.
b) Specify the type of endpoint by selecting UNI or ENNI from the dropdown list, and enter a name for the endpoint. For UNIs, you can also set bundling and multiplexing attributes.
c) Select the next endpoint and define its type, name, and attributes.
d) Click **Next**.
e) In the Manage Discovered Service: Service Details page, select the Type of service. The available types in the list are derived from the types of endpoints and UNI options you defined. For example, if you defined a UNI with All to one Bundling option, EPL, EP-LAN, and EP-Tree will be available in the list. If you define an ENNI, only Access EPL will be available in the list. You can go back and redefine your endpoints if necessary.
f) Give the service a name. Provide a description and specify a customer, if required.
g) For E-Tree EVCs, specify the role of each endpoint (root or leaf) in the Endpoint Designation table. The role you specify here must match the role that is configured on the device.
h) Click **Save**. The EVC will appear with its new name in the Circuits/VCs list and its status will be Created and Deployed.
i) You can now select the promoted EVC in the list and modify or delete it.

Step 8 For L3VPN services, do the following:

a) Give the service a name. Provide a description and specify a customer, if required, and click **Next**.
b) In the **Deployment Action** drop-down menu, specify the task (Preview or Deploy) that must be taken up when the VPN service promotion process is completed, and click **Next**.
c) Specify the UNI name, the MTU value, and whether service multiplexing should be enabled.

d) Click **Save**. The L3VPN service will appear with its new name in the Circuits/VCs list and its status will be Promote Successful.
e) You can now select the promoted L3VPN service from the list and modify or delete it.

Step 9 For MPLS TE Tunnel services, do the following:

a) Give the service a name if required. Provide a description and specify a customer, if required, and click **Next**.
b) Click **Save**. The MPLS TE Tunnel service will appear in the Circuits/VCs list and its status will be Promote Successful.
c) You can now select the promoted MPLS TE Tunnel service from the list and modify or delete it.

Note Default values for affinity and priority are re-configured in the modify flow after promotion of a tunnel.

MPLS TE tunnels discovered with lockdown on working path will lose the lockdown upon being modified and promoted.

Modify a Circuit/VC

You can modify circuits/VCs that are in the following provisioning states: Defined, Deployed, Failed, or Discovered. For more information about the provisioning states, see Circuit or VC States, on page 620.

Note You cannot change the UNI or endpoint selections. However, you can change the name of the UNI. If you want a different device to be an endpoint, you must delete the circuit/VC and create a new one.

For E-LAN and E-TREE EVCs, you can add or delete endpoints (sites).

To modify a circuit/VC:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2 From the toolbar, click **Device Groups** and then select the required group.

Step 3 Click the **Circuits/VCs** tab and then click the radio button for the circuit or VC you want to modify.

Step 4 From the **Circuits/VCs** pane toolbar, click the pencil (**Modify**) icon.

The Provisioning Wizard opens and displays information for the selected circuit or VC.

Step 5 Edit the circuit or VC as required, and then redeploy it. See Provision EVCs in a Carrier Ethernet Network, on page 507 and Provision Circuits in an Optical/DWDM Network, on page 526.

Activate a Circuit (Optical)

You can activate an optical circuit to determine if the traffic is passing through it. You can activate circuits that are discovered and deployed in the network. Also, the admin status of the circuit must be Down.

Step 1 From the left side bar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Device Groups** button and select the device group within which the required circuit/VC was created.

Step 3 In the **Circuits/VCs** tab, locate the optical circuit that you want to activate and click the information icon to access its Circuit/VC 360 view.

Step 4 Choose **Actions** > **Activate** to enable the traffic to pass through the optical circuit.

Note You can also activate the optical circuit from the Circuit/VC Details window and from the multilayer trace view. See View Circuits/VCs, on page 626 and Trace and Visualize the Full Route of Circuits/VCs, on page 676.

Step 5 Redeploy the optical circuit.

You can also choose to deactivate the optical circuit to stop the traffic passing through it. Ensure that the circuit is discovered and deployed in the network and the admin status of the circuit is Up. Click **Actions** > **Deactivate**.

Restore a Circuit (Optical)

You can restore an optical circuit when it encounters multiple successive failures and reroute the failed circuit over a new route.

You can restore or revert optical circuits that meet the following conditions:

- Circuit's provisioning state is Deployed or Discovered.
- The Restoration attribute for the circuit is set to true.
- The Revert mode for the circuit is set to manual or automatic.

To restore an optical circuit:

Step 1 From the left side bar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Device Groups** button and select the device group that contains the failed optical circuit.

Step 3 In the Circuits/VCs tab, locate the failed optical circuit and click the information icon to access its Circuit/VC 360 view.

Step 4 Choose **Actions > Restoration Actions > Upgrade Restore** to upgrade the failed optical circuit to an active route and delete the old route where the failure occurred.

Note You can also restore the failed optical circuit from the Circuit/VC Details window and from the multilayer trace view. See View Circuits/VCs, on page 626 and Trace and Visualize the Full Route of Circuits/VCs, on page 676.

Upgrade restore option will be disabled for circuits which are non-revertible.

When restoration is enabled , if required you will be allowed to add constraints.

On NCS2K devices for OCH-Trail WSON circuits the restoration status parameter is set to **Restored** only if the circuit is configured as **Revertive**.

You can also choose to revert the optical circuit to its original route when the route is recovered from the failure. Click **Actions > Restoration Actions > Manual Revert**.

Revert a Circuit (Optical)

You can revert an optical circuit to its original route when the route has recovered from a failure. This feature is available for all SVO circuits that are provisioned or discovered in Cisco EPN Manager.

To revert an optical circuit:

Step 1 In the left side bar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Device Groups** button and select the device group that contains the failed optical circuit.

Step 3 In the **Circuits/VCs** tab, locate the failed optical circuit and click the information icon to access its **Circuit/VC 360** view.

Step 4 Choose **Actions > Restoration Actions > Manual Revert** to upgrade the failed optical circuit to an active route and delete the old route where the failure occurred.

If the NE-Disconnected alarm on a working path or a restored path is not cleared, the circuit fails to revert. You can view the reason for the failure under the **History** tab.

On NCS2k SVO devices for OCH-Trail and OCH-NC circuits, the default number of retry attempts for **Restoration** and **Revert** is 12 and the default duration between retry attempts is 5 minutes.

You can change the default number of restoration and revert attempts using the **/opt/CSCOlumos/conf/optical-mp.properties** file. Use the parameter **restorationRestoreAttempts** to change the number of restoration attempts and **restorationRevertAttempts** to change the number of revert attempts.

Reroute a Circuit (Optical)

You can reroute a circuit to its working path or protected path so that you can perform network maintenance activities without interrupting the service. The reroute operation is available for all WSON circuits that are provisioned or discovered in Cisco EPN Manager.

Note The reroute operation is not available for circuits that has the restoration status as "Restored" or "Revertible".

Promote the discovered circuit before initiating re-route.

Step 1 From the left side bar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Device Groups** button and select the device group within which the required circuit/VC was created.

Step 3 In the **Circuits/VCs** tab, locate the optical circuit that you want to reroute and click the information icon to access its Circuit/VC 360 view.

Step 4 Choose **Actions** > **Reroute Actions** > **Working Path** or **Protected Path** to reroute the traffic through the working path or protected path defined for the circuit.

Note You can also reroute the optical circuit from the multilayer trace view. See Trace and Visualize the Full Route of Circuits/VCs, on page 676.

Repair a Circuit (Optical)

You can manually repair and resync a circuit path when a circuit is restored but remains in **Partial** state due to a fiber disconnect. This feature is available for all SVO circuits that are provisioned or discovered in Cisco EPN Manager.

To repair an optical circuit:

Step 1 In the left side bar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click the **Device Groups** button and select the device group that contains the failed optical circuit.

Step 3 In the **Circuits/VCs** tab, locate the failed optical circuit and click the information icon to access its Circuit/VC 360 view.

Step 4 Choose **Actions** > **Maintenance Actions > Repair** to repair the failed optical circuit on the same path where the failure has occurred.

It takes approximately 10 minutes for the repair to take place. If the circuit is not repaired, a description of why it failed is listed under the **History** tab.

If the **NE-Disconnected** event on a working path is cleared, you do not need to manually delete and repair orphan cross-connection circuits in the Circuit/VC 360° page. Any orphan cross-connection circuit that is associated with a disconnected node is automatically deleted. If the **Discovery State** of the circuit remains **Partial** after the orphan cross-connection circuit is deleted, the circuit is automatically repaired and resynced without the need to do it manually.

Compare and Reconcile Provisioned and Discovered Versions of a Circuit/VC

Note This functionality is supported for Carrier Ethernet VCs, Circuit Emulation, and Serial services only.

When you provision a circuit/VC using Cisco EPN Manager, the relevant CLI commands are configured on the devices participating in the circuit/VC. After a circuit/VC is provisioned using Cisco EPN Manager, the system discovers the provisioned circuit/VC from the network. In some cases, there might be differences between the provisioned CLI and discovered CLI, for example, if a configuration change was made on a device after provisioning. Cisco EPN Manager allows you to compare the provisioned and discovered versions of a circuit/VC and generate a reconciliation report showing the differences. Based on the report, you can decide whether to keep the discovered version or revert to the provisioned version. If you choose to keep the discovered version, the circuit/VC in the Cisco EPN Manager is synched with this version.

The comparison and reconciliation functionality is accessed from the circuit/VC tables.

The functionality is disabled if the circuit/VC discovery state is Missing or the provisioning state is None, In Progress, or Delete Succeeded.

To compare and reconcile a circuit/VC:

Step 1 Open a table of circuits/VCs, either the full table of all circuits/VCs in the system (**Inventory > Other > Circuits/VCs and Network Interfaces)** or a list of circuits/VCs for a specific device group (**Maps > Network Topology > Circuits/VCs tab > Circuits/VCs link**).

Step 2 In the circuits/VCs table, locate and select the required circuit/VC.

Step 3 Choose **Actions > Reconciliation Report**.

A comparison report is displayed, showing the differences in provisioned and discovered attributes on specific devices in the circuit/VC. If there are no differences between the provisioned and discovered attributes, "No data available" is displayed in the report.

Note For EVPN based services, EVI parameters like RD, RT, and Control Word are excluded from the report.

Step 4 After you have reviewed the report, you can choose to save the discovered version to the database as the current version of the circuit/VC or to revert to the provisioned version. At the top of the page, select the Provisioned or the Discovered radio button and click **Reconcile**.

If you chose Provisioned, the circuit/VC will be redeployed and the attribute values of the original provisioned circuit/VC will be configured on the devices. If you chose Discovered, the discovered circuit/VC will be stored in the database and this version will replace the original provisioned version. The provisioning status will indicate whether the reconcile action was successful.

Step 5 If the system requires your input to complete the reconciliation, the Provisioning Wizard will be launched. Fill in the required information and redeploy the circuit/VC.

Initiate a Protection Switch Action on a Circuit (Optical)

You can initiate a protection switch action on an optical circuit to switch over the traffic from one path to another path. For example, the traffic in an optical circuit is flowing through a working path and the working path is damaged. You can initiate a protection switch action on this circuit to switch over the traffic from the working path to the protected path.

Note You can initiate protection switch actions only on optical circuits in which the 1+1 or 1+1+R protection type is enabled. For more information about the protection types, see Circuit Section Reference for OTN Circuit Types, on page 545.

To initiate a protection switch action:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

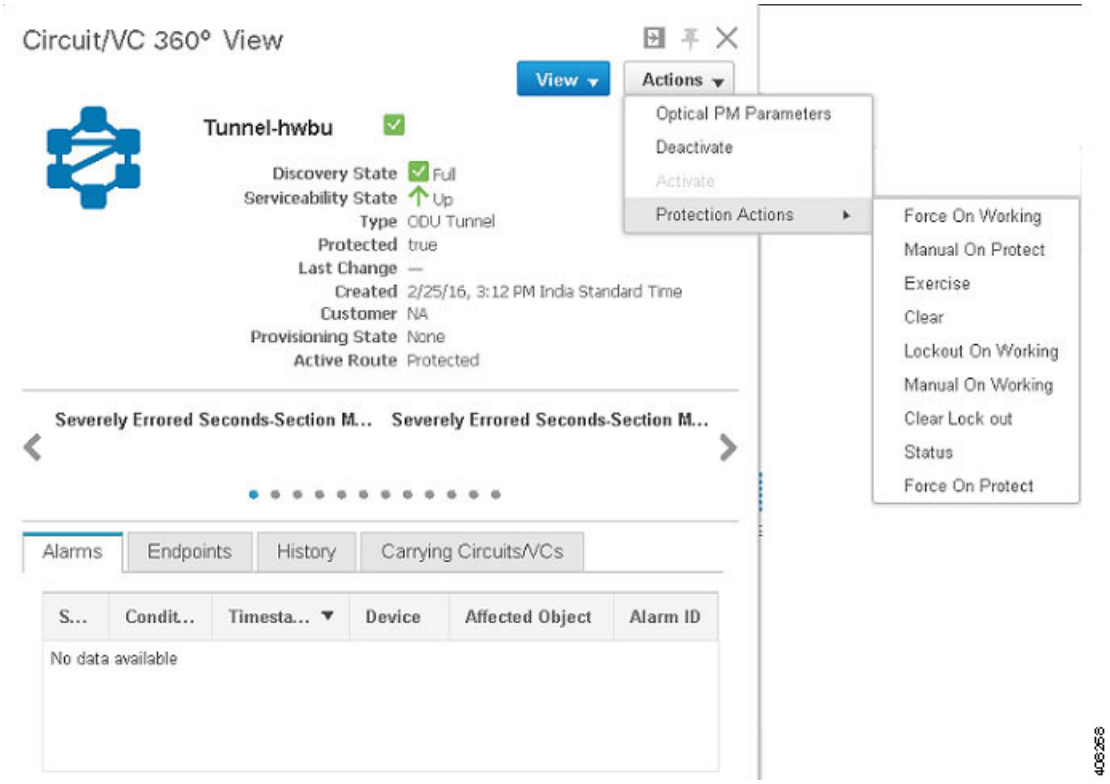
Step 2 Click **Device Groups**, and then select the location in which the required circuit/VC was created.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 On the **Circuits/VCs** tab, locate the required circuit/VC and click the *i* icon next to the circuit/VC name. The Circuit/VC 360 view appears in a separate popup window.

Step 6 Choose **Actions** > **Protection Actions**, and then choose the required protection switch action.



The following table provides a detailed description of each of the protection switch actions.

Protection Switch Action	Description	Applicable when:
Force On Working	Configures the working path to carry traffic over the network.	The current state of the protection switch action is 'Manual On Protect' or 'Manual On Working'.
Manual On Protect	Switches the traffic manually from the working to the protected path.	There is no protection switch action initiated on the circuit.
Clear	Clears the protection switch state on the circuit.	The current state of the protection switch action is not 'Lockout On Working'.
Exercise	Checks if an ODU subcontroller is ready for a protection switch.	There is no protection switch action initiated on the circuit.
Manual On Working	Switches the traffic manually from the protected path to the working path.	There is no protection switch action initiated on the circuit.

Lockout On Working	Configures an ODUk subcontroller as a locked out resource in the ODU subcontroller group. Locks the circuit so that its traffic cannot be switched to the working path.	The current state of the protection switch action is not 'Lockout On Working'.
Clear Lock out	Clears the 'Lockout On Working' switch state for the circuit.	The current state of the protection switch action is 'Lockout On Working'.
Status	Displays the details of ODU subcontroller group and the protection switch state specified in the AID.	Available for all protected optical circuits.
Force On Protect	Configures the protected path to carry traffic over the network.	The current state of the protection switch action is 'Manual On Protect' or 'Manual On Working'.

Resynchronize a Circuit/VC

When there is any issue with circuit/VC, such as primary or discovery state is down, or the link between the participating devices is missing, you can resynchronize the circuit. Cisco EPN Manager synchronizes the circuit with the participating devices on a best-effort to resolve the issue.

To resynchronize the circuit/VC:

Step 1 Access one of the following pages:

- Circuit/VC 360 View. See Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 629.
- Circuit/VC Details Window. See Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window, on page 635.
- Multi-Layer Trace View. See Trace and Visualize the Full Route of a Circuit, on page 197

Step 2 Choose **Actions** > **Resync**.

The discovery state of the circuit will change to Resync when the resync action is in progress. Once the action is completed, the discovery state will change to Full or Partial.

Service Discovery Resync

You can resync the supported serial services, IOT CEM and IOT CEM variants X.21 C 3794, MPLS-TE, CE, L3VPN, SR-TE, CEM over T1/E1/E3/T3/SONET/SDH services, if there are any conflict changes on the devices.

In the service 360 view area, from the Action drop-down list, choose Resync to update the related entities, that is, you can perform the service resync pertaining to a particular service.

Note View the current status in the Discovery State field. The resynced status and timestamp are displayed in the Manual Resync State.

Delete a Circuit/VC

You can choose to either delete or force delete a circuit/VC.

You can delete circuits/VCs that are in the following provisioning states: Create/Modify Succeeded or Create/Modify/Delete Failed.

As a network administrator you can force delete an MPLS TE tunnels and Layer 3 link for the selected services in the circuit VCs window. This option will be available when there is a failure in previous delete operation or a Service is in missing state.You can force delete circuits/VCs that are in the Delete Failed provisioning state. When you force delete a circuit/VC, it is removed from the Cisco EPN Manager database. The circuit/VC will not appear in the circuit/VC tables.

Caution However, the force delete option may not remove the configurations from all the devices participating in the circuit/VC. You may need to manually clean up the devices.

Note The force delete option is not available for optical circuits.

To delete or force delete a circuit/VC:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

The network topology window opens.

Step 2 From the toolbar, click **Device Groups** and then select the required group.

Step 3 Click the **Circuits/VCs** tab and then click the radio button for the circuit or VC you want to delete.

Step 4 From the **Circuits/VCs** pane toolbar, do one of the following:

- From the X (Delete) icon drop-down list, choose **Force Delete**. A confirmation message is displayed. A corresponding job is created in the Jobs dashboard and you can monitor the progress. After the job is completed, the circuit/VC is removed from the Cisco EPN Manager database.
- Click the X (**Delete**) icon. The Provisioning Wizard opens and displays information for the selected circuit or VC.

Step 5 Click **Next** to go to the **Service Details** page.

Step 6 In the Deploy area, specify what you expect the delete operation to accomplish:

- Delete the circuit or VC from devices and Cisco EPN Manager—This will remove the configurations from all the devices participating in the circuit or VC and will also remove it from the database. The circuit or VC will not appear in the circuit and VC tables and no history will be available for it.

- Delete the circuit or VC from devices only—The circuit and VC history will remain in the database but all relevant configurations will be removed from the devices participating in the circuit or VC.

Note These options are only available in the wizard when deleting an EVC/OVC with "failed" status, for example, "Create failed," Modify failed," and so on.

Step 7 In the **Deployment Action** field:

- Choose **Preview** to view the configurations that will be deployed to the relevant devices before the actual deployment.
- Choose **Deploy** to deploy the changes without previewing them.

Step 8 Click **Submit**.

- If you selected **Preview** in the previous step, a Preview Config page is displayed. If you are satisfied with the changes, click **Deploy**.
- If you selected **Deploy** in the previous step, the configurations are deployed to the devices immediately.

A confirmation message is displayed when the deployment is complete.

To view the details of configuration, configuration errors, rollback configuration, and rollback configuration errors for each device participating in the circuit/VC, click the *i* icon next to the **Provisioning** column in the Deleted Circuits/VCs tab in the extended tables. The *i* icon is available for all provisioning states, except None. For information about how to access the extended tables, see View Detailed Tables of Alarms, Network Interfaces, Circuits/VCs, and Links from a Network Topology Map, on page 175.

Note If you delete a circuit on the device that is being managed by Cisco EPN Manager through another EMS or directly through the CLI, NETCONF, TL1 interfaces without using Cisco EPN Manager, the circuit is not deleted automatically in Cisco EPN Manager. You must use the **Delete** or **Force Delete** option to delete the circuits.

Delete or Force Delete an L3VPN Service

You can delete or force delete L3VPN services that were originally created using Cisco EPN Manager. L3VPN services that were only discovered but not created using Cisco EPN Manager cannot be deleted.

To delete or force delete an L3VPN service:

Step 1 In the left pane, choose **Maps** > **Network Topology**.

Step 2 In the Circuits/VCs panel, click the **Circuit/VCs** link to display all services in Cisco EPN Manager.

Step 3 Select the service that you want to delete or force delete. You can type the service's name in the **Name** filter to filter out the required L3VPN service and click the X (**Delete**) icon.

Step 4 Alternately, from the **Circuits/VCs** pane toolbar, do one of the following::

a) Choose the service that you want to delete and click the X (**Delete**) icon.

The Provisioning Wizard opens and displays information for the selected circuit or VC.

Click Next to proceed to the Service details .

The L3VPN Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN.

b) From the X (Delete) icon drop-down list, choose **Force Delete**. A confirmation message is displayed. A corresponding job is created in the Jobs dashboard (**Administration** > **Dashboard** > **Job Dashboard** > **User Jobs** > **Force Delete Circuit**) and you can monitor the progress. After the job is completed, the Layer 3 link is removed from the Cisco EPN Manager database.

Also, use the Force Delete option when you are not able to proceed with the Service deletion from the GUI.

Step 5 Select **Submit** to preview the configuration that is to be pushed on the device.

Step 6 Review the configuration and click **Deploy** to confirm. A confirmation message is displayed when the deployment is complete.

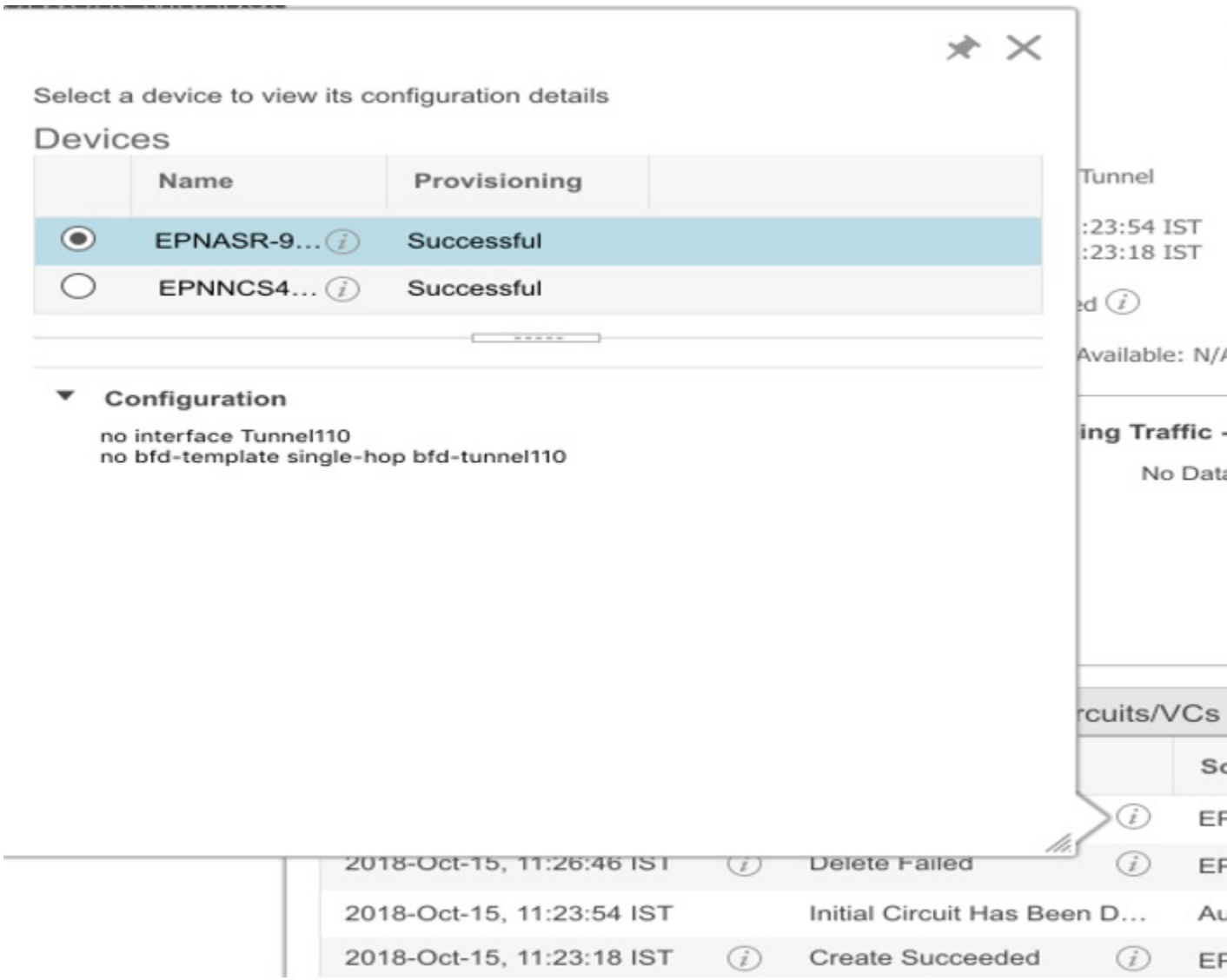
The selected L3VPN service is deleted from the device.

Note If the selected L3VPN service uses integrated routing and switching (BVI/virtual interfaces), then deleting the L3VPN service automatically deletes the associated BVI/virtual interface from the device. The BGP and VRF settings associated with the L3VPN service are also deleted.

Step 7 To verify that the selected L3VPN was deleted from the device, view the complete list of L3VPN services from the Circuits/VCs list.

Step 8 To view the device configurations of the force deleted services, click the *i* icon next to the Provisioning column in the **History** tab in the **Deleted Circuit/VCs** tab. In the Circuit /VC 360* View window, click the *i* icon that is available for all provisioning states, except **None** to view the configuration details of the selected devices.

Figure 15: Circuit /VC 360 View*



Delete an L3VPN Service Endpoint

You can delete L3VPN service endpoints for L3VPN services created using Cisco EPN Manager. Endpoints associated with L3VPN services that are discovered but not created using Cisco EPN Manager cannot be deleted.

To delete an L3VPN service endpoint:

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 In the Circuits/VCs panel, click the **Circuit/VCs** link to display all services in Cisco EPN Manager.

Step 3 Select the service that you want to delete. You can type the service's name in the **Name** filter to filter out the required L3VPN service.

Step 4 Click the pencil**Modify** icon.

The L3VPN Provisioning wizard displays the VRFs, endpoints, and other details associated with the selected L3VPN.

Step 5 Choose **Delete Endpoint** and click **Next**.

Step 6 Choose the IP endpoints that must be disassociated from the selected L3VPN service. For single endpoint VRFs, deleting the endpoints turns the VRF ineffective and the VRF then acts as a dangling VRF. To associate newer endpoints with this ineffective VRF, you need to further edit the VRF's attributes.

Step 7 Click **Next** to preview the configuration that will be pushed to the device.

Step 8 Review the configuration and click **Deploy** to confirm and deploy your changes to the device.

The selected L3VPN service endpoint is deleted from the device.

Delete or Force Delete an MPLS TE Service

You can delete or force delete MPLS TE services that are in the following provisioning states: Planned, Succeeded, Failed, or None. For more information about the provisioning states, see Circuit or VC States, on page 620.

Note You cannot delete an MPLS TE service if it is being used by a CEM service or a Carrier Ethernet circuit/VC.

Step 1 From the left pane, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location in which the required circuit/VC was created.

Step 3 Close the **Device Groups** popup window.

Step 4 In the **Network Topology** window, click **Circuits/VCs**.

Step 5 In the **Circuits/VCs** tab, click the Circuits/VCs hyperlink located below the list of circuits/VCs.

Step 6 In the displayed table of circuits/VCs, select the MPLS TE service that you want to delete.

Step 7 Click the delete icon or Force Delete to open the Provisioning Wizard and display information for the selected MPLS TE service.

Step 8 From the **Deployment Action** drop-down list, choose one of the following option:

- **Preview**—View the configurations that will be deployed to the relevant devices before the actual deployment.
- **Deploy**—Deploy the changes without previewing them.

Step 9 Click **Submit**.

- If you selected Preview in the previous step, Cisco EPN Manager displays a Preview Config page. If you are satisfied with the changes, click **Deploy**.
- If you selected Deploy in the previous step, Cisco EPN Manager deploys the configurations to the devices immediately.

To view the details of device configuration of the force deleted services, click the *i* icon next to the Provisioning column in the **History** tab in the **Circuit/VC 360*** window. The *i* icon is available for all provisioning states, except **None**.

Cisco EPN Manager displays a confirmation message when the deployment is complete.

Manage Provisioned Network Interfaces

Cisco EPN Manager provides a table of interfaces that have been provisioned as network interfaces (UNIs or ENNIs) so that you can view details for and manage network interfaces independently of provisioned circuits/VCs. The table provides information about each network interface, including its identifying information, the device it belongs to, the actual interface on the device, and the number of services in which the network interface is currently participating.

You can view:

- The network interfaces in a specific device group (from the Network Topology window).
- All network interfaces managed by Cisco EPN Manager (from the Inventory menu).

You can edit a network interface by clicking the **Edit** button. This launches the wizard where you can make changes to the network interfaces as required. Keep in mind that if the network interface is associated with multiple services, your edit operation will affect all of those services.

You can delete a network interface as long as it is not participating in any circuits.

Step 1 To view and manage the network interfaces that belong to a specific device group:
a) In the left sidebar menu, choose **Maps** > **Topology Maps** > **Network Topology**.
b) Click the **Device Groups** button and select the required group.
c) In the **Circuits/VCs** tab, click the **Network Interfaces** hyperlink (below the table).

Step 2 To view and manage all network interfaces managed by Cisco EPN Manager, choose **Inventory** > **Other** > **Network Interfaces**.

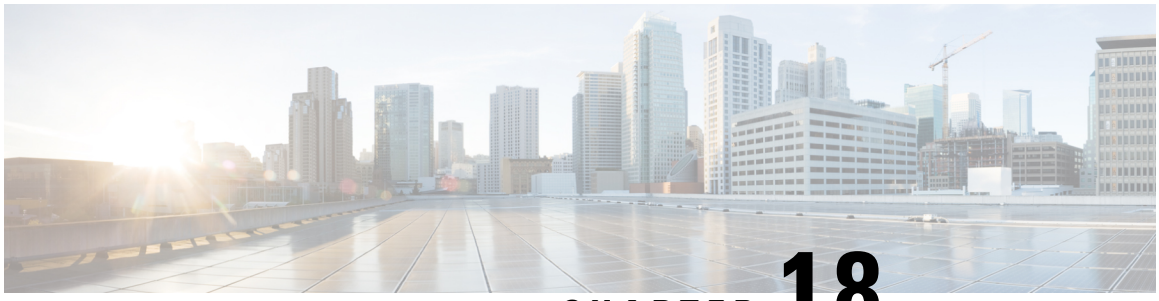
Delete Network Interfaces

From the Network Interfaces table, you can delete a UNI/ENNI if it is not currently participating in any circuits.

To delete a network interface:

Step 1 In the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.
Step 2 Click the **Device Groups** button and select the required group.
Step 3 In the Circuits/VCs tab, click the Network Interfaces hyperlink to display the Network Interfaces table.

Step 4 Select the network interface you want to delete and click the **Delete** button. If the network interface is participating in one or more circuits/VCs, the Delete button will be disabled. In the No. of Circuits/VCs column, you can see the number of circuits/VCs in which the network interface is included.



CHAPTER 18

Monitor and Troubleshoot Circuits/VCs

Check Circuits/VCs for Faults

Cisco EPN Manager provides several ways to see, at a glance, if there are any problems with circuits/VCs:

- Circuit list—The colored icon to the left of each circuit/VC name indicates the primary state of the circuit/VC. If the primary state indicates a problem with the circuit/VC, you can access detailed alarm information for the circuit/VC, as described below.
- Circuit/VC 360 view—The Alarms tab in the Circuit/VC 360 view shows all alarms on all devices over which the circuit/VC is configured. Click the information icon next to the circuit/VC name to access the Circuit/VC 360 view.
- Alarm Table—The alarm table shows all alarms for all devices, for a specific device group, or for a specific device. Choose **Monitor > Monitoring Tools >Alarms and Events** to access the alarm table. If you have identified an alarm in the Circuit/VC 360 view, you can get more details about the alarm in the alarm table. You can search for the alarm or for the device/link that generated the alarm using the quick filter or the advanced filter.Each alarm in the table can be expanded to show detailed information about the alarm, including which circuits/VCs are affected by the alarm.
- Circuit/VC Overlay in the Network Topology—When a circuit/VC is selected in the Circuits/VCs list, it is represented on the network topology as an overlay on top of the existing topology. If the alarm is on a specific device, the alarm badge will appear on the device as usual. If the alarm is on the link between the circuit/VC endpoints, the alarm badge will appear on the link.
- Multi-layer trace for optical circuits—See Trace and Visualize the Full Route of Circuits/VCs, on page 676.

Identify Which Circuits/VCs are Affected by a Specific Fault

To identify which circuits/VCs are affected by a specific fault:

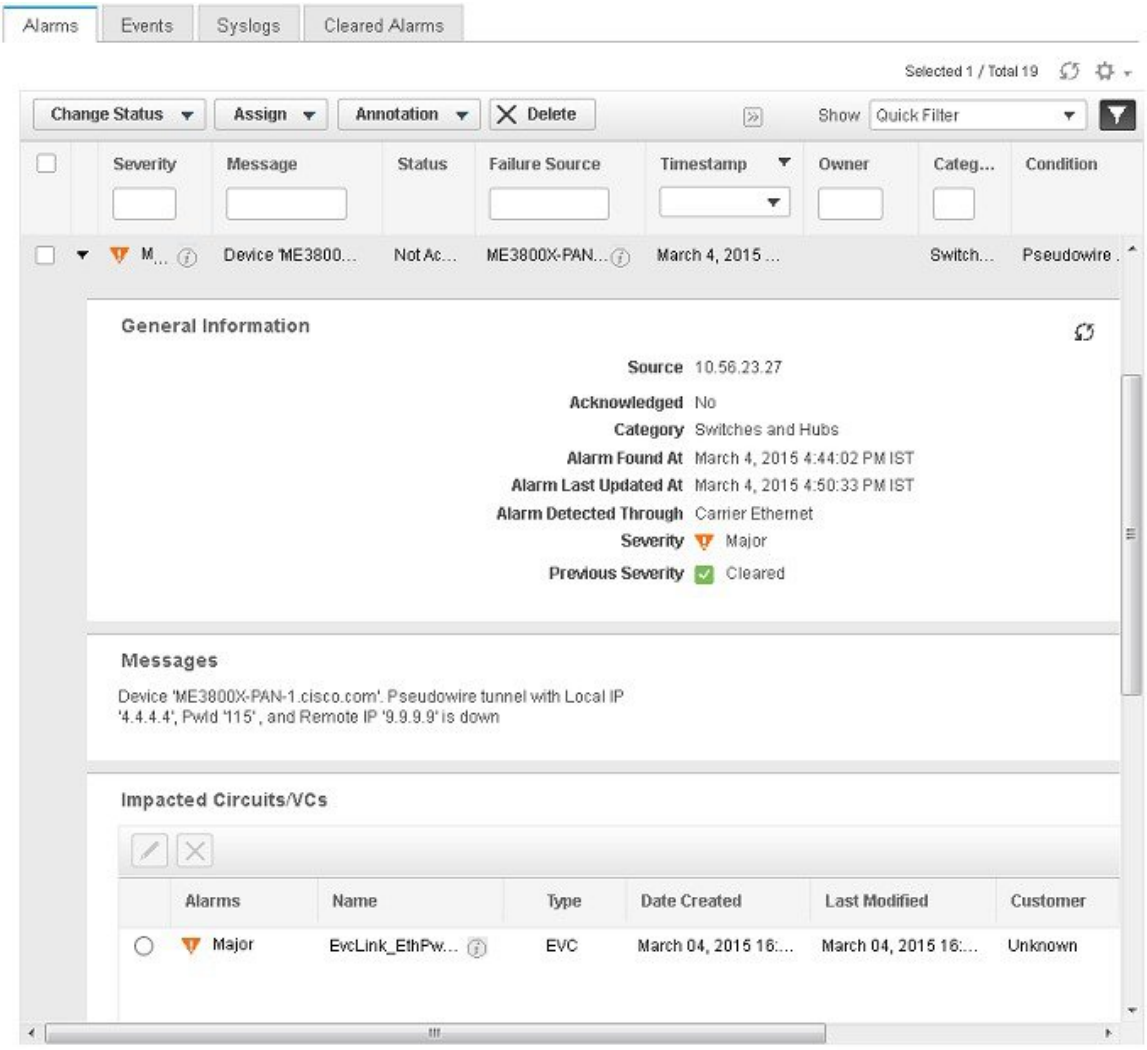
Step 1 From the left side bar, choose **Monitor > Monitoring Tools > Alarms and Events**.

Step 2 In the alarm table, locate the required alarm. You can use the simple or advanced filters to locate the alarm, if necessary.

Step 3 Click on the arrow to the left of the row to expand the row and display the alarm details.

Step 4 Locate the Impacted Circuits/VCs pane. All circuits/VCs that are affected by the selected alarm are listed in this pane, with basic information for each circuit/VC. You can access the Circuit/VC 360 view to get more details about the circuit/VC by clicking the *i* icon.

Step 5 If necessary, you can modify or delete the circuit/VC from the Impacted Circuits/VCs pane by selecting a circuit/VC and clicking the Modify or Delete button. This opens the Provisioning Wizard. See Modify a Circuit/VC, on page 644 and Delete a Circuit/VC, on page 651 for more information.



Get More Information About a Circuit/VC Failure

Cisco EPN Manager provides information about why the provisioning operation of a circuit/VC has failed so that you can troubleshoot the issues. In the Circuits/VCs table, you can identify problems with a circuit/VC by looking at the Provisioning state and the Serviceability and Discovery states. If there has been an error during the provisioning of a circuit/VC and the circuit/VC could not be created, the Provisioning state will be Create Failed. You can click the *i* icon in the Provisioning column to see the configuration of the devices involved in the failure, as well as details about the specific error(s) that occurred.

For optical circuits, the combination of Serviceability state Down and Discovery state Partial can indicate a problem with the circuit. In this case, you can click the *i* icon in the Serviceability column to see the reason that the Serviceability state is Down.

Note Information about a circuit/VC failure can also be accessed from the Circuit/VC 360 view. See Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 629.

To view additional information about a circuit/VC provisioning failure from the Circuits/VCs table:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 In the **Network Topology** window, click the **Circuits/VCs** tab, and then click the **Circuits/VCs** hyperlink. A table listing all the circuits is launched in a separate window.

Step 3 Locate the circuit for which the provisioning operation has failed. The Provisioning state will be **Create Failed**.

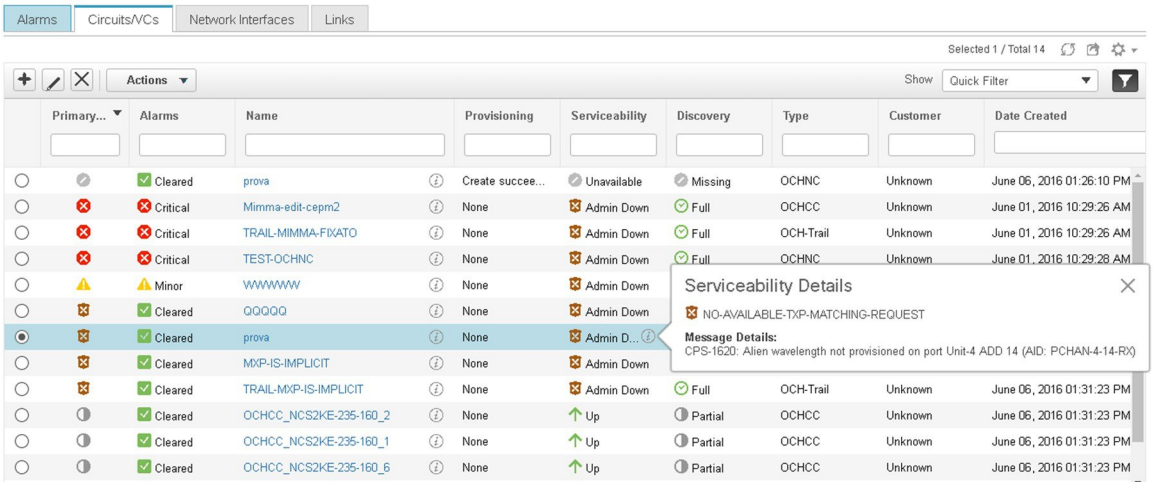
Step 4 Click the *i* icon next to the **Provisioning** column. A popup window is displayed and lists the devices on which the provisioning errors occurred.

Step 5 Select a device to see its configuration and error details.

Step 6 Click the *i* icon next to the **Serviceability** column to view the **Serviceability Details** data pop-up window that displays information about why the provisioning operation has failed for the circuit.

Note The *i* icon is available only if the serviceability status is down and the discovery status is partial.

For optical circuits, if the Serviceability state is Down and the Discovery state is Partial, click the *i* icon next to the Serviceability column to view the Serviceability Details data pop-up window that displays information about why the circuit's serviceability state is Down. You can also view the Serviceability Details data pop-up window from the Circuit/VC 360 view. For information about how to access the Circuit/VC 360 view, see Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 629.



Troubleshoot a Service Failure Using OAM Commands

Cisco EPN Manager provides the ping and traceroute features to troubleshoot service failures. You can use OAM commands to access these features and monitor the connectivity and path between two endpoints in a

service. You can then isolate and resolve the failure. The technologies that are supported for the different IOS devices are:

- MPLS LSP, Pseudowire, and CFM: Cisco IOS-XE devices and Cisco IOS-XR devices
- MPLS Bidirectional TE Flex LSP and VRFs: Cisco IOS-XE devices

The launch points for the OAM command vary based on:

- Technology type—Launching from Network Devices Table, on page 663 (This launch point for OAM commands is supported only for the **MPLS LSP** technology.)
- Service type—Launching from Circuit 360, on page 663
- Event type—Launching from Alarm Browser, on page 664

You can perform ping or traceroute using the OAM commands to troubleshoot a service failure. See Perform a Ping or Traceroute Using OAM Command, on page 665

Launching from Network Devices Table

To launch MPLS LSP technology OAM command from Network Devices table:

Step 1 Choose **Inventory** > **Device Management** > **Network Devices**.

Step 2 In the Network Devices table, select a MPLS enabled device.

Step 3 Click the >> icon above the Network Devices table and select **OAM Commands**.

Launching from Circuit 360

If you are launching OAM command from the Service/Circuit 360, the service type is the criteria that determines the technology that is supported. See Overview of Circuit/VC Discovery and Provisioning, on page 479 to know in detail about the different service types.

To launch OAM command from Circuit 360:

Step 1 Choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 In the **Network Topology** window, click the **Circuits/VCs** tab and click the *i* icon next to the circuit to view the Circuit 360. Based on the service type of the circuit you selected, the supported technology OAM commands as mentioned in this table are displayed.

Service Type for which you can launch the OAM command:	Technology supported
Carrier Ethernet	• Segment Routing LSP • Pseudowire • CFM

Service Type for which you can launch the OAM command:	Technology supported
Circuit Emulation (CEM)	• MPLS LSP • Pseudowire • Bidirectional TE (Flex LSP)
L3VPN	• MPLS LSP • VRF
Bidirectional TE Tunnel (Flex LSP)	• MPLS LSP • Bidirectional TE (Flex LSP)

Step 3 Click **Actions** and select the ***Technology*** **OAM** that is displayed for the service type you chose.

Launching from Alarm Browser

If you are launching OAM command from the alarm browser, the event type is the criteria that determines the technology that is supported.

To launch OAM command from an alarm browser:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**.

Step 2 In the Alarms table, select an alarm with an event type listed in the "Event Type for which you can launch the OAM command" column in this table.

Technology supported	Event Type for which you can launch the OAM command:
MPLS Bidirectional TE Tunnel (Flex LSP)	• mplsTunnelUp • mplsTunnelDown • mplstunnelReoptimized • ROUTING-MPLS_TE-5-LSP_UPDOWN • MPLS_TE-5-TUN • MPLS_TE-5-LSP
VRFs in L3VPN	• mplsL3VpnVrfUp • mplsL3VpnVrfDown • mplsL3VpnNumVrfRouteMaxThreshCleared • mplsL3VpnVrfNumVrfRouteMaxThreshExceeded • mplsL3VpnVrfRouteMidThreshExceeded
Pseudowires in Carrier Ethernet and Circuit Emulation	• cpwVcDown • cpwVcUp • XCONNECT-5-PW_STATUS Down • L2-L2VPN_PW-3-UPDOWN
CFM in Carrier Ethernet	• E_CFM-3-REMOTE_MEP_DOWN_TIME_OUT • L2-CFM-6-MEP_CHANGE

Step 3 Click **Troubleshoot** above the Alarms table and select **OAM Commands**.

Perform a Ping or Traceroute Using OAM Command

To perform a ping or traceroute or multipath (only for SR) using OAM command:

Step 1 Launch the ***Technology*OAM Command** window. See Troubleshoot a Service Failure Using OAM Commands, on page 662 for the OAM command launch points for the supported technologies.

Step 2 Based on the launch point, select the required fields as displayed in this table for the selected technology type.

Technology Type	Launched from Alarm Browser	Launched from Service/Circuit 360
Pseudowire	Details are auto-populated	From the **Pesudowire Endpoint** drop-down list, choose the endpoint participating in the service.
LSP	From the **Destination LDP ID** drop-down list, choose the LDP ID of the destination endpoint participating in the service.	Specify the **Source** and **Destination** from the drop-down lists. In the **Destination** field, • If a LDP enabled device is selected, then Ping and Traceroute options are enabled. • If SR enabled device is selected, then Ping, Traceroute, Multipath, Nil FEC Ping and Nil FEC Traceroute options are enabled. (Nil FEC options are enabled only if Label, OutputInterface and NextHop fields are populated)
MPLS Bidirectional TE Tunnel (Flex LSP)	Choose the tunnel's path as **Active**, **Working**, or **Path-Protect** for which you want to perform a ping or traceroute. Cisco EPN Manager performs the ping or traceroute on both directions, that is, from headend to tailend and vice versa.	Choose the tunnel's path as **Active**, **Working**, or **Path-Protect** for which you want to perform a ping or traceroute. Cisco EPN Manager performs the ping or traceroute on both directions, that is, from headend to tailend and vice versa.
VRF in L3VPN	From the **End Points** drop-down list, choose the endpoint of another VRF that belongs to the same VPN.	From the **Source End Points** and **Destination End Points** drop-down lists, choose the source and destination endpoints of another VRF that belongs to the same VPN.

Technology Type	Launched from Alarm Browser	Launched from Service/Circuit 360
CFM in Carrier Ethernet	From the **Destination MEP ID** drop-down list, choose the MEP ID of the destination endpoint participating in the service.	From the **Source MEP ID** and **Destination MEP ID** drop-down lists, choose the MEP IDs of the source and destination endpoints participating in the service.
SR TE		From the **Policy Name** drop-down list, choose a policy. Note: This option is enabled for devices configured over static and dynamic SR policies or EVPN technology.

Step 3 Choose **Actions** > **Ping** to perform a ping, choose **Actions** > **Traceroute** to perform a traceroute, and choose **Actions** > **Multipath** to perform a multipath action.

The results of the ping, traceroute and multipath commands are displayed in the following formats:

Note
- For MPLS bidirectional TE tunnels, the results are displayed for both directions, that is, from headend to tailend and vice versa.
- For Pseudowire, the results are displayed in visual and tabular formats and as raw data.

- Visual—The service with the endpoints and its hops is displayed on a map. Hover your mouse cursor over the endpoints to view additional information such as the outgoing and incoming interfaces.

Note The traceroute command results for all the technologies are displayed in visual format.

- Table Data—The information such as the outgoing and incoming interfaces, device names, and labels of the endpoints participating in the service are displayed in a tabular format.

Note The traceroute and multipath command results are displayed in tabular format.

- Raw Data—The information about the endpoints participating in the service is displayed as unformatted source data.

Note Ping, traceroute and multipath command results are displayed as raw data.

Use EOAM Templates to Troubleshoot EVCs

Cisco EPN Manager provides several predefined templates that can be used to monitor the connectivity and performance of virtual connections (VCs) in a Carrier Ethernet network. To use these templates, choose **Configuration > Templates > Features & Technologies > CLI Templates > System Templates - CLI**. See Perform EOAM Connectivity and Performance Checks, on page 432 for more information.

Run a Performance Test on a Circuit/VC

When you run a performance test, Cisco EPN Manager connects to the network elements to provide real-time data. To get historical information, see View Performance Metrics and Reports for Circuits/VCs, on page 675.

- Performance Test Based on Y.1564 for EVCs, on page 667
- Performance Test Based on Y1731 for EVCs, on page 670
- Performance Test for Optical Circuits, on page 671
- Performance Test for Circuit Emulation Services, on page 673

Performance Test Based on Y.1564 for EVCs

CE performance tests verify the correct configuration and performance of CE EVCs at the time of activation. You can also use the CE performance tests to troubleshoot an EVC that is already in operation.

The Y.1564 Ethernet service activation or performance test methodology allows turning up, installing, and troubleshooting Ethernet-based services. Using this test, you can verify the service configuration and performance from UNI to UNI. This ensures that the SLA will be met according to the bandwidth profile purchased, and the promised class of service.

These tests provide complete validation of Ethernet service-level agreements (SLAs) in a single test. Using a traffic generator performance profile, you can create the traffic based on your requirements. The network performance, such as throughput, loss, and availability, are analyzed using Layer 2 traffic with various bandwidth profiles.

Note You can only run performance tests on EVCs that are configured on the network and discovered by Cisco EPN Manager.

Supported Devices

The Y.1564 performance test is supported on the following devices running IOS 15.4(S) or IOS XE 3.12S and higher:

- List of devices that can be specified as either source or destination:
  - Cisco ASR 920 routers
  - Cisco ASR 907 routers with RSP3 as both source and destination (loopback)

- Cisco ASR 903 routers with RSP2, RSP3 as both source and destination (loopback)
- Cisco ASR 901 routers
- Cisco ASR 9000 series devices (as loopback)
- Cisco NCS 4201 devices
- Cisco NCS 4202 devices
- Cisco NCS 4206 devices

Note The Cisco NCS 4206 devices are supported as both source and destination starting from version 16.5 and onwards. However, for devices with versions preceding 16.5, they are only supported as a destination.

- Cisco NCS 4216 devices
- Cisco NCS 540 devices (as a loopback)
- Cisco NCS 5500 devices (as loopback)
- Cisco ME 1200 devices

- List of devices that can be specified as destination (loopback) only:
  - Cisco NCS 4206 devices
  - Cisco ASR 903 routers RSP/RSP1

Running a Y.1564 Performance Test

To run a Y.1564 performance test on an EVC, do the following:

Before you begin

If you want to run a Y.1564 performance test on an EVC that resides on a ME1200 device, enter the following QoS configuration on both the source and destination interfaces before you run the test:

```
Interface <interface-name>
qos map tag-cos pcp 0 dei 0 cos 0 dpl 0
qos map tag-cos pcp 0 dei 1 cos 0 dpl 1
qos map tag-cos pcp 1 dei 0 cos 1 dpl 0
qos map tag-cos pcp 1 dei 1 cos 1 dpl 1
qos map cos-tag cos 0 dpl 0 pcp 0 dei 0
qos map cos-tag cos 0 dpl 1 pcp 0 dei 1
qos map cos-tag cos 1 dpl 0 pcp 1 dei 0
qos map cos-tag cos 1 dpl 1 pcp 1 dei 1
```

Step 1 Choose **Maps** > **Topology Maps** > **Network Topology** to open the **Network Topology** page.

Step 2 From the toolbar, click **Device Groups** to open the **Device Groups** pop-up window.

Step 3 Locate and click the device group that contains the circuit/VC you want to test, then close the pop-up window.

Step 4 Click the **Circuits/VCs** tab, locate the relevant service, and then click its *i* (**information**) icon to open its **Circuit/VC 360** view.

Step 5 From the top right corner of the view, choose **Actions** > **Y.1564 Test** to open the Y.1564 performance test settings page.

Note This test can also be initiated from the **Circuit/VC** tab in a device's **Device 360** view and the **Circuits/VCs & Network Interfaces** page. See View a Device Group's Circuits/VCs, on page 638 and View Circuits/VCs, on page 109.

Step 6 Configure the settings for the performance test:

a) In the **Test Mode** field, specify whether this will be a one- or two-way test by clicking the appropriate radio button. Note that in the case of a two-way test, loopback will be created on the service instance of the destination device.

b) In the **End Points** area, choose the source and destination device, interface, and EFP ID from the drop-down lists.

c) In the **Service Configuration Test** area, specify the duration of each iteration, the size of packets to be generated, and the rate at which traffic will be generated.

- If you choose the **CIR/EIR** radio button, specify values (in kilobits per second) for the Committed Information Rate (CIR) and Excess Information Rate (EIR). The CIR is the long-term average transmission rate, whereas the EIR is the long-term average excess transmission rate.
- If you select the **Color Aware Test** check-box, specify the Class of Service (CoS) values between 0 to 7 for the **Conform Action** and **Exceed Action**. The CoS values must be set different for **Conform Action** and **Exceed Action** to differentiate and prioritize the traffic. Also, you may specify the values (in kilobytes per second) for the Committed Burst Size (CBS) and Excess Burst Size (EBS) to define the committed or excess traffic that can be transmitted in bursts at temporary rates above the CIR.

  Note The **Color Aware Test** check-box will be enabled only for FPGA enabled devices with 10G ports. “Color Aware” is used to describe the mode where the customer is marking each frame as green or yellow, and the network takes this marking into account at the bandwidth profiler and traffic policer.

- If you check the **Step Load CIR** check box, the test will generate traffic at four different levels: 25, 50, 75, and 100% of the CIR value you specify. Note that this option is not available if the CIR is set to a value lower than 8 kbps.
- If you choose the **Custom Rates** radio button, 1000 kbps is set by default. Change this value, if necessary.
- If you are running a one-way performance test, you can only specify a custom traffic rate.

d) In the **Service Acceptance Criteria** area, enter the highest acceptable frame loss ratio value (in percent) in the **FLR** field.

- If you also want to set a frame transfer delay (FTD) and frame delay variation (FDV) value, check the corresponding check box and then enter the appropriate value (in milliseconds).

  Note The **FTD** and **FDV** check-boxes will be enabled only for FPGA enabled devices with 10G ports.

- If any of the thresholds you set are exceeded during the performance test, the EVC will be deemed as having failed the test.

e) (Optional) In the **Frame Settings** area, specify values for the following parameters:

- IP version—IPv4 or IPv6
- Inner and outer VLAN ID—Identify the source and destination VLAN ID you want to test

Step 7 Click **Run Test**.

When the test is completed, the results are displayed at the bottom of the Y.1564 performance test settings page.

Performance Test Based on Y1731 for EVCs

The Y.1731 Performance Monitoring (PM) provides a standard ethernet PM function that includes measurement of ethernet frame delay, frame delay variation, frame loss, and frame throughput measurements specified by the ITU-T Y-1731 standard and interpreted by the Metro Ethernet Forum (MEF) standards group. Using this test, you can verify the delay and loss measurements such as the delay and loss probe status, delay and loss probe availability, two-way delay, two-way jitter, loss forward, and loss backward for your circuit/VC.

Note This performance test is supported on Cisco IOS, IOS-XR and IOS-XE devices.

Before you begin

Following are the prerequisites that must be met before you run a performance test based on Y.1731 for a circuit/VC:

- The circuit/VC, along with the participating devices, on which you want to run the performance test, must be operationally up.
- Ensure that the MEP ID matches the domain name for all the devices participating in the circuit/VC.

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups**, and then select the location that contains the circuit/VC you want to test.

Step 3 In the **Network Topology** window, click **Circuits/VCs**.

Step 4 Locate the required circuit/VC, and then click the information icon to access its Circuit/VC 360 view.

Step 5 Choose **Actions** > **Y.1731 Test**.

Note The performance test can also be initiated from the circuit/VC details window and from the expanded list of circuits/VCs. See View a Device Group's Circuits/VCs, on page 638 and View Circuits/VCs, on page 109.

Step 6 Choose the required source and destination devices and their corresponding interfaces.

Step 7 From the **CoS** drop-down list, choose the priority of the probe. The default value is 0.

Step 8 Choose the required measurement type. The options are **Delay**, **Loss**, and **Loss & Delay**.

Note While delay measurement is done using Delay Measurement Message (DMM) probe, loss measurement is done by Synthetic Loss Measurement Message (SLM) probe. In case of ASR 1K devices, delay measurement using Loss Measurement Message (LLM) probe is only supported.

Step 9 If required, define the advanced performance test parameters as follows:

- Probe Length—Choose the length of the probe in seconds. For example, if the probe length is set to 30 seconds, the statistical data is collected every 30 seconds and displayed in the test results area.

- Packet Size—Enter the size (in bytes) of the packets that you want to send for each probe.
- Burst Interval—Choose the burst interval in seconds. This defines the time interval between two sets of packets that are sent for a probe.
- Packet Interval—Choose the packet interval in milliseconds. This defines the time interval between two packets that are sent for a burst.
- Packet Count—Enter the number of packets that will be sent for a burst.

  For example, if the burst interval, packet interval, and packet count are set to 30 sec, 1000 ms, and 10 respectively, 10 packets will be sent in the interval of 1000 ms between one packet and the next packet. Once all the 10 packets are sent, there will be an interval of 30 sec after which the next set of 10 packets will be sent.

Step 10 Click **Run Test**. When the test is completed, the results will be displayed at the bottom of the Performance Test page, under the Test Results area.

Performance Test for Optical Circuits

Cisco EPN Manager performance test for optical circuits is based on the ITU-T recommendations as defined in G.709 and G.798.

Cisco EPN Manager supports the following performance tests for Optical Circuits:

- Optical Performance Monitoring Parameters, on page 671
- Run PRBS Test on Circuits (ODU UNI), on page 672

Optical Performance Monitoring Parameters

Optical Performance Monitoring Parameters monitor the quality of optical signals and are used to measure the average optical power transmitted and received between end points in optical circuits. From these measurements, you can derive critical network performance parameters such as channel presence verification, channel wavelength, ASE noise, optical signal power, optical signal to noise ratio (OSNR), and electrical signal to noise ratio (eSNR) per channel. You can then use these parameters to manage the network reliability and quality of service.

Follow the steps below to view the performance monitoring parameters for an optical circuit:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Select the device group that contains the circuit/VC you want to test.

Step 3 In the Circuits/VCs pane on the left, locate the required service and click the *i* icon to access its Circuit/VC 360 view.

Step 4 Choose **Actions > Optical PM Parameters** .

Note The performance test can also be initiated from the circuit/VC details window and from the expanded list of circuits/VCs. See View a Device Group's Circuits/VCs, on page 638 and View Circuits/VCs, on page 109.

Step 5 Select an optical monitoring type based on which the performance data will be displayed. For more information about the optical monitoring types and the associated performance counters, see Performance Counters for Optical Monitoring Policies, on page 958.

Step 6 Choose the performance monitoring time interval as 15 minutes or 24 hours to collect the performance data from the device.

Step 7 Specify the time interval to automatically refresh the performance data.

Step 8 Click **Auto Refresh**. The performance data for the circuit is displayed as a tabular representation. For the detailed descriptions of the performance data, see Performance Counters for Optical Monitoring Policies, on page 958.

Based on the time interval specified to refresh the performance data, the newly retrieved data is displayed at the beginning of the table. For example, if the time interval specified is 10 seconds, the performance data is automatically refreshed every 10 seconds and the newly retrieved data is displayed at the beginning of the table. The table displays the last 20 entries of the performance data retrieved.

Run PRBS Test on Circuits (ODU UNI)

PRBS test is supported for OTN Circuits of type ODU UNI. PRBS bit error count measures the reliability of the link between the endpoints. This test is supported for NCS4K-20T-O-S cards. When PRBS test is run between 2 endpoints (ODU Controller or sub-controller), the source device sends a bit pattern through one or more midpoints (intermediate controller or sub-controller) and the same bit pattern is received by the destination device, the test results can be viewed from both the endpoints. You can also run the PRBS test on a controller, configuring the other endpoint as a loopback, source, or source-sink.

For information on configuring PRBS on an ODU controller, see Configure PRBS on ODU Controllers, on page 358.

To run a PRBS performance test for an optical circuit:

Step 1 From the left sidebar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Select the device group that contains the circuit/VC of type ODU UNI you want to test.

Step 3 In the Circuits/VCs pane on the left, locate the required service and click the *i* icon to access its Circuit/VC 360 view.

Step 4 Choose **Actions** > **PRBS Test**.

Step 5 To assign roles to the endpoints, in the **Endpoint** table, click the endpoint's role and select one of the following options from the drop-down list:

- SOURCE—To set this role to either A or Z side.
- SINK—To set this role to either A or Z side.
- SOURCESINK—To set this role either to A side, Z side, or both.
- INVALID—To disable PRBS on the endpoint.

Step 6 To assign patterns to the endpoints, in the **Endpoint** table, click the endpoint's pattern and select the desired pattern from the drop-down list.

Following patterns are supported for NCS4K-20T-O-S cards:

- PRBS 31
- PRBS 31 Inverted
- PRBS 11
- PRBS 11 Inverted

Step 7 To change the loopback mode, in the Loopbacks table, click the endpoint's or midpoint's loopback mode and select one of the following options from the drop-down:

- NO_LOOPBACK—For testing without loopback.
- INTERNAL—For testing within the same network.
- LINE—For testing across different network.

Step 8 In the **Test Results** area, select the endpoint from the **Sink Controller** drop-down list.

Step 9 Click one of the following **Interval** radio button, to set the time interval to collect the data from the device:

- Current (every 10 seconds)—Displays past 15 minutes results every 10 seconds.
- 15 Minutes—Displays past 15 minutes historic performance data.
- 1 Day—Displays past 1 day historic performance data.

Step 10 Click **Go**.

Step 11 Click **Auto Refresh**. The test result for the endpoints is displayed as a tabular representation which includes bit error count, packets lost and found timestamps and packet lost and found counts.

Based on the time interval specified to refresh the test, the newly retrieved data is displayed at the beginning of the table. For example, if the time interval specified is 10 seconds, the data is automatically refreshed every 10 seconds and the newly retrieved data is displayed at the beginning of the table.

Performance Test for Circuit Emulation Services

Bit error rate test (BERT) allows you to test cables and diagnose signal problems in the field. This testing mechanism is supported on the Cisco NCS 42xx Series (T1/E1 Ports and T3/E3 Ports). This test generates a specific pattern onto the outgoing data stream of a circuit controller and then analyzes the incoming data stream for the same pattern. The bits that do not match the expected pattern are counted as bit errors.

The bit error rate is determined by comparing the erroneous bits received and the total number of bits received. You can view and analyze the total number of error bits transmitted and the total number of bits received on the circuit. You can retrieve error statistics anytime during the test.

The following table lists the test patterns that are supported in Cisco NCS 42xx series (T1/E1 Ports and T3/E3 Ports) devices.

BERT Pattern	Description
2^11	Pseudo-random repeating test pattern that consists of 2,048 bits.
2^15	Pseudo-random repeating test pattern that consists of 32,767 bits.
2^20-O151	Pseudo-random repeating test pattern that consists of 1,048,575 bits.
2^20-O153	Pseudo-random repeating test pattern that consists of 1,048,575 bits.
2^23	Pseudo-random 0.151 test pattern that is 8,388,607 bits in length.
2^9	Pseudo-random 0.151 test pattern that is 511 bits in length.

To run a BERT performance test for a CEM circuit:

Step 1 From the left sidebar, choose **Inventory** > **Others** > **Circuits/VCs & Network Interfaces**.

Step 2 In the **Circuits/VCs** tab, locate the required CEM service and click the *i* icon to access its Circuit/VC 360 view. In the Circuit/VC 360 view, choose **Actions** > **Performance Test** > **BERT**.

Alternatively, you can reach this page through **Maps** > **Topology Maps** > **Network Topology** and in the **Circuits/VCs** pane, access the Circuit/VC 360 view of the required CEM circuit.

Step 3 In the **Test** tab, select the test direction, source, and destination.

For easy understanding, the pictorial representation of the test in the circuit is displayed, once the source and destination are selected.

Step 4 To refresh the test data automatically for a defined time interval, in the **Settings** area, enter the time interval in minutes.

Step 5 Select the pattern from the **BERT Pattern** drop-down list.

Step 6 Click **Run Test**. The test result is displayed in the **Test Results** area. See View and Export the Results of the Performance Test on Circuit Emulation Services, on page 674

Step 7 To terminate the test, in the **Settings** area, click **Stop** and click **Clear Counters** to reset the values in the **Test Results** area.

In case of SONET interfaces, the **Clear Counters** button is disabled once you terminate the test.

View and Export the Results of the Performance Test on Circuit Emulation Services

At a time, BERT performance test can be performed on any number of CEM circuits but only one test can be performed on a single CEM circuit. The results of the BERT performance test on a CEM circuit is displayed in the **Test Results** area.

- At any point in time, the results of last run/currently running BERT performance test on a CEM circuit is displayed in the **Test Results** area in the **Test** tab.
- If the **Auto-refresh** is enabled (ON), then the test results are auto-refreshed at the specified time period.
- In the **Test Results** area:
  - No test results are displayed, when an Unmanaged Endpoint is chosen as destination for a test.
  - Two set of test results are displayed, each for an endpoint, when a Managed Endpoint is chosen as destination.
- Choose **Monitor** > **Performance Tests** > **BERTs**. Here, only a single entry for each CEM circuit is available and it shows either the last run/currently running test on that CEM circuit. Select the required CEM circuit to view its test results.
- To view the historical records of BERT performance results for a specific CEM circuit, in the **History** tab, select the required test from the **Test** drop-down list to view the configuration and its result.

You can export the results of a BERT performance test by clicking the Export icon at the top right corner of the **Test** and **History** tabs of the BERT page (from the Circuit/VC 360 view, choose **Actions** > **Performance Test** > **BERT**).

You can also export the list of BERT performance tests from the following pages:

- **Select BERT Test** pop-up window (from the BERT page, click the **History** tab, and then click the **Test** drop-down list to open the **Select BERT Test** pop-up window).
- BERT listing page (choose **Monitor** > **Performance Tests** > **BERTs**).

View Performance Metrics and Reports for Circuits/VCs

The Circuit/VC 360 view provides information about the circuit's recent history. Reports, on the other hand, can retrieve all historical data stored in the database. For real-time information, run a performance test (see Run a Performance Test on a Circuit/VC, on page 667).

View Performance Graphs in the Circuit/VC 360 View

The Circuit/VC 360 view contains graphs showing various aspects of the circuit/VC performance. This view is helpful if you want to see, at-a-glance, if there are any major issues with circuit/VC performance. For more information, see Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 629.

To access the Circuit/VC 360 view:

Step 1 From the left side bar, choose **Maps** > **Topology Maps** > **Network Topology**. The network topology window opens. See Visualize the Network Topology, on page 173 for a description of the Network Topology window and its functionality.

Step 2 In the Locations pane on the left, select the device group within which the required circuit/VC was created.

Step 3 In the Circuits/VCs pane, locate the required circuit/VC and click on the *i* icon next to the circuit/VC name. The Circuit/VC 360 view appears in a separate popup window.

Use Performance Reports to Monitor and Troubleshoot Circuits/VCs

Cisco EPN Manager provides extensive reporting capabilities that enable you to retrieve in-depth performance information for optical circuits and EVCs. The Report Launch Pad provides access to all Cisco EPN Manager reports. From the Report Launch Pad, you can create and save new reports, view current reports, open specific types of reports, schedule a report to run later, and customize the results of a report.

Choose **Reports > Report Launch Pad** in the left navigation pane to access the reports and the reporting functionality.

For information about Carrier Ethernet performance reports, see Carrier Ethernet Performance Reports, on page 283.

For information about Optical performance reports, see Optical Performance Reports, on page 296.

Use Service Performance Dashboard to Monitor Circuits/VCs

Service Performance dashboard provides a collection of graphical and tabular representation of Performance measurement for the selected circuit/VC over time. This information is available in the form of customized dashlets. The dashboard menu provides access to all the available Cisco EPN Manager dashboards.

From Service Performance Dashboard, you must select a circuit/VC from the Circuits/VCs drop-down list to view the following information (dashlets):

- Average availability of service endpoints over time.
- Incoming and outgoing traffic measured in bits per second, for services over a specified time period.
- Average delay between the service endpoints over time.
- Average packet loss ratio between the service endpoints over time.
- List of services with highest incoming and outgoing traffic.

To launch the dashboard for a specific service from its Circuit/VC 360 view, click **View** and then choose **Dashboard**.

For more information on the Service Performance dashboards and dashlets, see Service Performance Dashboard Overview, on page 5.

For more information on managing dashboards and dashlets, see Get Started With Cisco EPN Manager, on page 1.

Trace and Visualize the Full Route of Circuits/VCs

Use the Multilayer Trace view (MLT) to visualize a circuit in a graphical manner. This view displays the complete circuit span and service trace between two endpoints and can be used to trace the connectivity of a circuit by displaying the source node, destination node, and any intermediate nodes in graphical format.

Note the following:

- Multilayer Trace view is not supported for Multipoint Carrier Ethernet circuits/VCs, Serial - Raw Socket, and L3VPN services.
- You can launch the Multilayer Trace view for optical circuits only when LMP is configured on the A end device and also between devices participating in the optical circuit.
- For MPLS-TE and SR-TE tunnels, physical topology is required for the Multilayer Trace view, which means that the physical links must have been discovered using one of the supported protocols, for example, CDP or LLDP.

To trace and visualize the full route of a circuit:

Step 1 From the left side bar, choose **Maps** > **Topology Maps** > **Network Topology**.

Step 2 Click **Device Groups** and then select the location in which the required circuit/VC was created.

Step 3 On the Network Topology page, click **Circuits/VCs**. The list of circuits/VCs associated with the selected device group is displayed.

Step 4 Select a circuit/VC for which you want to view the full route. The overlay of the circuit is displayed on the map.

Step 5 Use one of the following ways to switch to the Multilayer Trace view:

- Click the **Multilayer Trace** hyperlink on the notification that appears right below the topology toolbar.

  Note The **Multilayer Trace** hyperlink appears only if the Multilayer Trace view is supported for the selected circuit/VC and if the primary state of the circuit/VC is not 'Missing'.

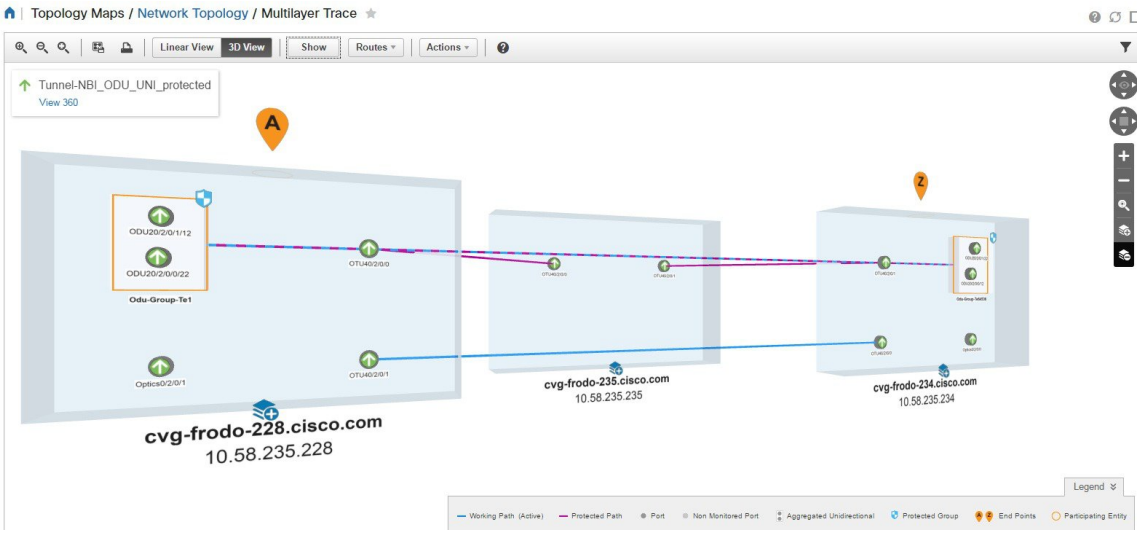
  You can view the partial multilayer trace even when a full route of a circuit/VCs is not completely modeled or if the route is broken. You can identify the root cause and the suggestions to overcome the error.

- Click the information icon adjacent to the circuit/VC to open the Circuit/VC 360 view, and then click **View>Multilayer Trace**.

The simplified three-dimensional view of the selected circuit/VC is displayed. In the simplified view, only the source and destination endpoints of the participating devices are displayed. You can choose to either expand or collapse the different layers in the circuit/VC. The animation of the route direction between the endpoints is displayed for some circuit types. For more information, see View Specific Information of a Circuit in a Multilayer Trace View, on page 679.

Note In the case of a device with a circuit being traversed more than once (more incoming and outgoing connections), the collapse option is disabled in both three-dimensional and linear views.

The following figure shows the simplified view of a circuit/VC with the expand and collapse options.



For more information about the details displayed in a three-dimensional view, see Three-Dimensional View of a Circuit V/C Trace, on page 679.

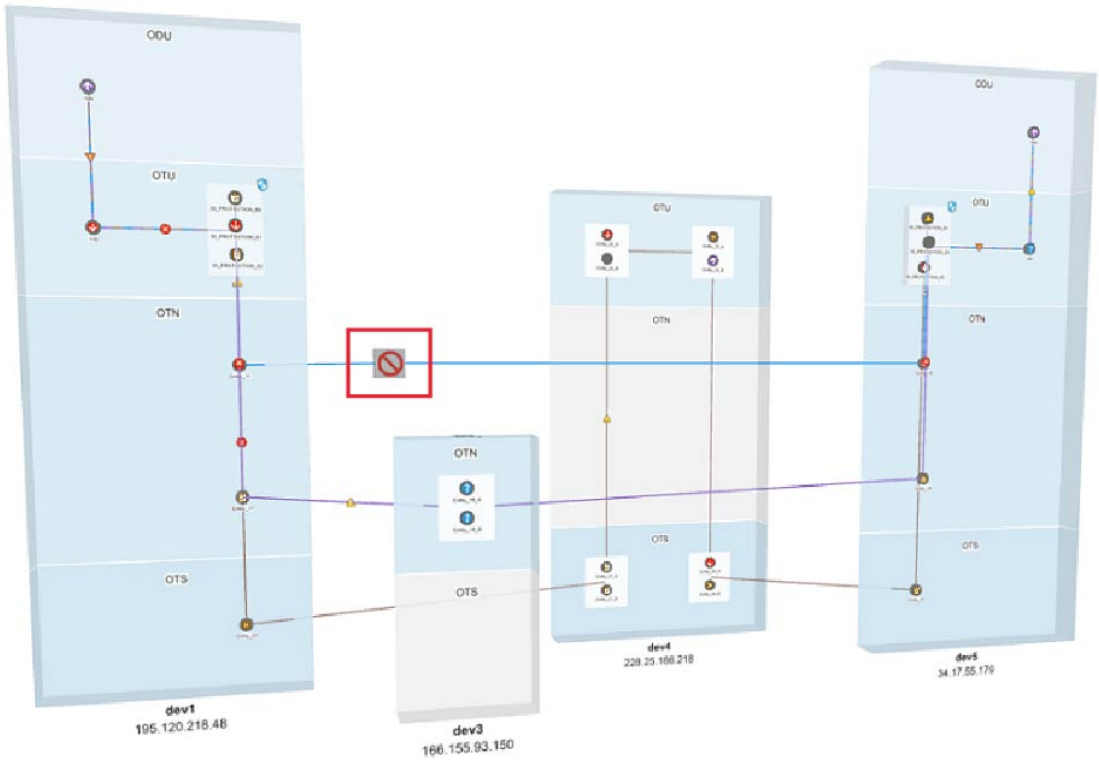
To switch to the linear view, click **Linear View**. For more information about the details displayed in a linear view, see Linear View of a Circuit/VC Trace, on page 679.

The Multilayer Trace view displays a graphical map that:

- Uses high-level span information such as NEs and links to display the circuit trace.
- Displays logical high-level view where the circuit is traced on the map using logical links, for example, OCHCC circuits use OCH trail links for the trace.

- Displays physical high-level view where the circuit is traced on the map using physical links, for example, OCHCC circuits use OTS links for the trace.
- Displays badges on the devices that represent the most severe alarm on the device, irrespective of the selected circuit. The alarm badges within the trace view show the alarms on each entity (for example, a link, node, or point).
- Highlights links according to the high-level view that you select.
- Highlights the layers with different shades and displays border lines that delineate the different layers in the circuit. If a layer is not applicable for a device, that layer appears in gray color.
- Displays a collapsible legend that lists the different icons and descriptions of each icon displayed in the Multilayer Trace view.
- For optical circuits, indicates whether the devices or links in the circuit have Shared Risk Resource Groups (SRRGs) assigned to them. Click on the SRRG label on the link or device to see a list of all the SRRGs on that link/device. The SRRGs are color-coded based on whether they are the default on the device, assigned, or yet to be assigned. Click on the question mark icon to see the legend.
- For OCHCC circuits, displays the LMP links between the source or destination node and the DWDM controller.

If one or more devices participating in the circuit/VC is not part of your virtual domain, the Multilayer Trace will be partial. Instead of the inaccessible device, you will see an inaccessible device icon in the Multilayer Trace view (as shown in the figure below).



Three-Dimensional View of a Circuit V/C Trace

This is the default view. It displays a three-dimensional view of the full route of a circuit/VC. For information about how to access this view, see Trace and Visualize the Full Route of Circuits/VCs, on page 676.

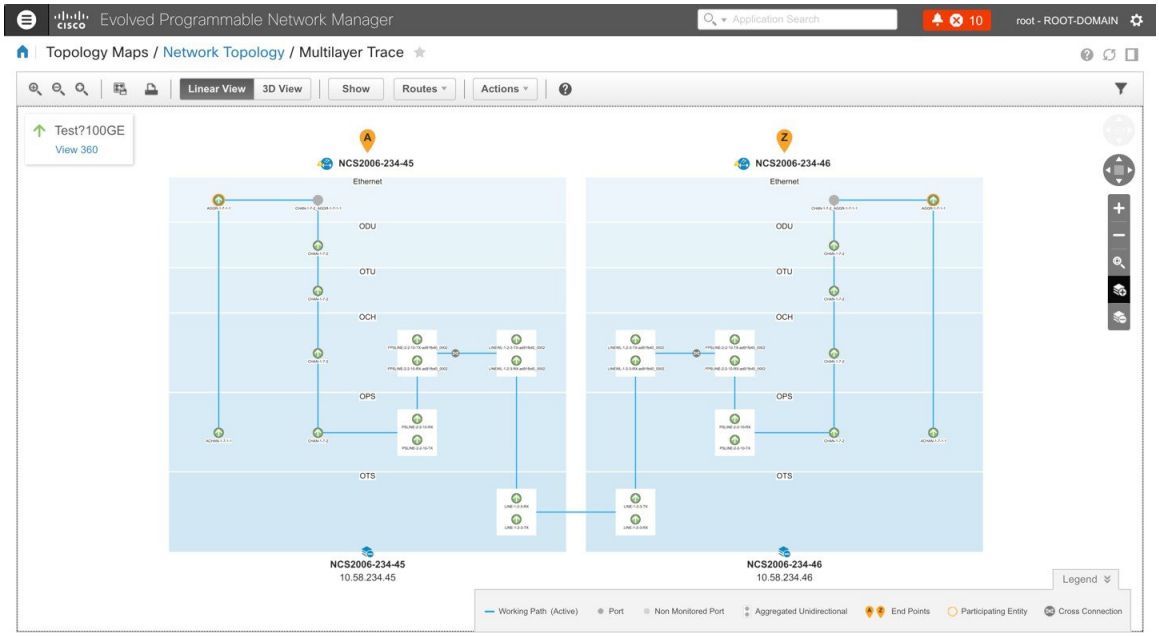
To know about the navigation controls in the three-dimensional view, click the help icon in the tool bar. The Navigation Controls data popup window shows the mouse, MAC Trackpad, and keyboard controls to pan, zoom, and rotate in this view.

Note The MAC Trackpad controls are displayed only for MAC users.

Linear View of a Circuit/VC Trace

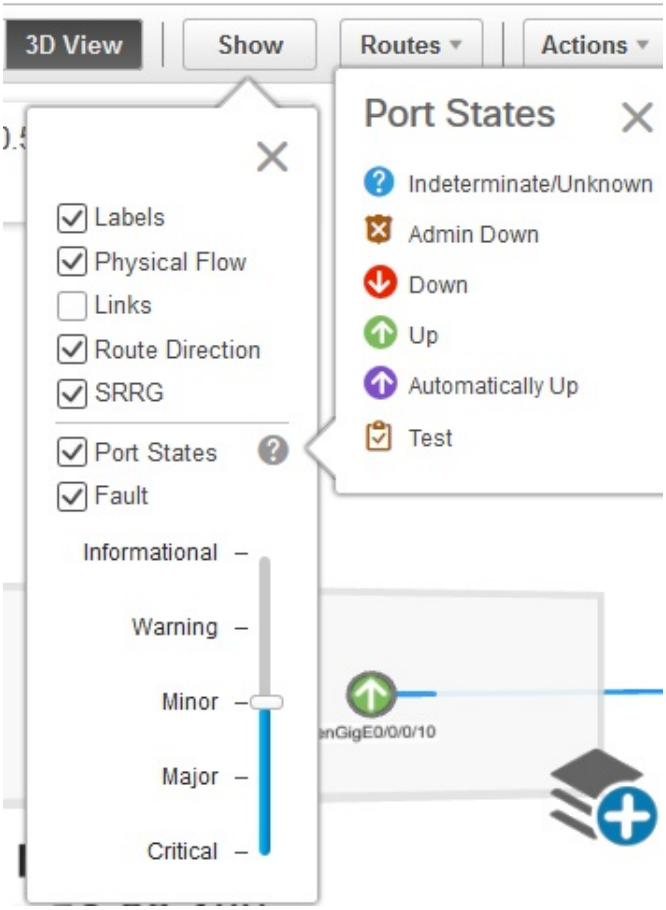
Using the linear view, you can trace and visualize the route of a circuit/VC in a two-dimensional view. For information about how to access this view, see Trace and Visualize the Full Route of Circuits/VCs, on page 676.

This view displays only one path of the circuit at a time. Choose **Route**, and then select **Working**, **Protected**, or **Restored** to view the required path in the circuit trace. The path options will vary depending on the type of circuit/VC you selected.



View Specific Information of a Circuit in a Multilayer Trace View

In the multilayer trace view of a circuit, you can choose what information you want to view by enabling the specific check box from the **Show** menu. You can choose to view the labels, physical flows, links, route directions, SRRG, port states, power levels, span loss, and faults in the circuit. The check boxes vary depending on the type of circuit/VC you selected.



You can view either the alarm status or the primary state of the ports. For a list of the port primary state icons and a description of the states, see Port or Interface States, on page 97.

The **Route Direction** check box to view the animation of the route direction in a circuit, will be enabled by default, only for those circuits which have non-symmetrical paths:

- Unidirectional circuits with path from A to Z. For example, Unidirectional TE Tunnels.
- Bidirectional non-symmetrical circuits with the paths from A to Z and Z to A not being the same. For example, a Carrier Ethernet or a CEM circuit traversing over a unidirectional TE Tunnel.

Note The **Route Direction** check box will not appear in the **Show** menu for circuits that have exactly the same path from A to Z and Z to A i.e., bidirectional symmetrical circuits.

By default, the route direction from A to Z end will appear. To view the animation in the opposite direction, click the  icon. But this icon will be enabled only for those circuits (bidirectional non-symmetrical circuit) that has different A to Z and Z to A paths. For example, a Carrier Ethernet or a CEM circuit traversing over two different unidirectional TE Tunnels. The switch icon does not appear for these circuits:

- Unidirectional circuits with path from A to Z. For example, Unidirectional TE Tunnels.

- Bidirectional symmetrical circuits with the paths from A to Z and Z to A being exactly the same. For example, Bidirectional Core Routed TE Tunnel (or Flex LSP).

When you apply filter to the layers, the **Route Direction** check box gets disabled depending on the chosen layer. Once disabled, it does not get auto-enabled and you have to manually enable the check box to view the route direction animation again.

In case of a partially discovered circuit or a problematic/unsupported circuit configuration, the default route direction from A to Z might not launch. But these circuits may have a potential Z to A direction, which traverses a different path. Click the **Change Endpoints** hyperlink to configure the endpoints to launch the multilayer trace view in the opposite direction.

Actions You Can Perform from the Multilayer Trace View

You can do the following from the Multilayer Trace view:

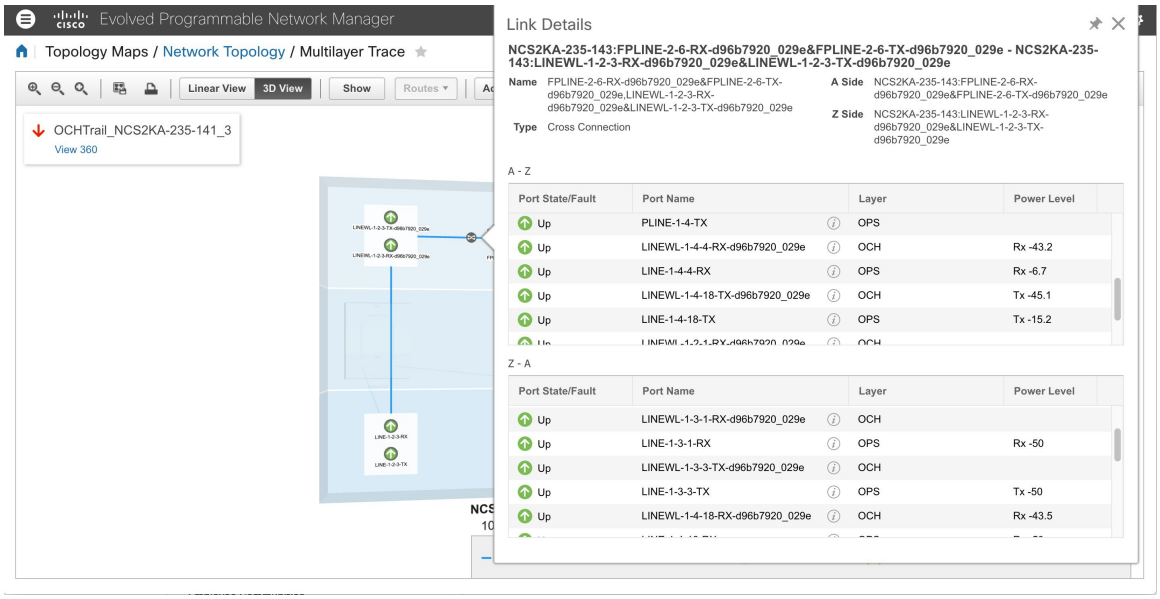
- Choose **Show**, and then check the appropriate check boxes to view the labels, physical flows, links, port states, power levels, span loss, and faults in the circuit. For more information, see View Specific Information of a Circuit in a Multilayer Trace View, on page 679.
- Hover over a link, interface, or circuit to view the link name, card name, or the circuit name respectively.

Note Card name is not displayed for cross-connection interfaces in the circuit.

- Click the **View 360** hyperlink that appears right below the toolbar in the Multilayer Trace to open the Circuit/VC 360 view. See Get Quick Information About a Circuit/VC: Circuit/VC 360 View, on page 629.
- Click the Port icon on the circuit trace to open the Interface 360 view. See Get a Quick Look at a Device Interface: Interface 360 View, on page 103.
- Click the device name or device IP address that appears at the top of the device to open the Device 360 view. See Get Basic Device Information: Device 360 View, on page 84.
- Click a link in the Multilayer Trace to open the Link 360 view. See Get a Quick Look at a Specific Link: Link 360 View, on page 186.
- Click the Cross Connection icon on the circuit trace to open the Link Details pop up window.

Note The Cross Connection icon appears on the links where internal ports are used by the circuit/VC. The internal ports are not displayed in the Multilayer Trace view.

The following figure shows the Link Details pop up window that lists the affected internal ports, port status, layer, and power levels. These details are listed for all the affected internal ports in both directions, that is from A side to Z side and vice versa.

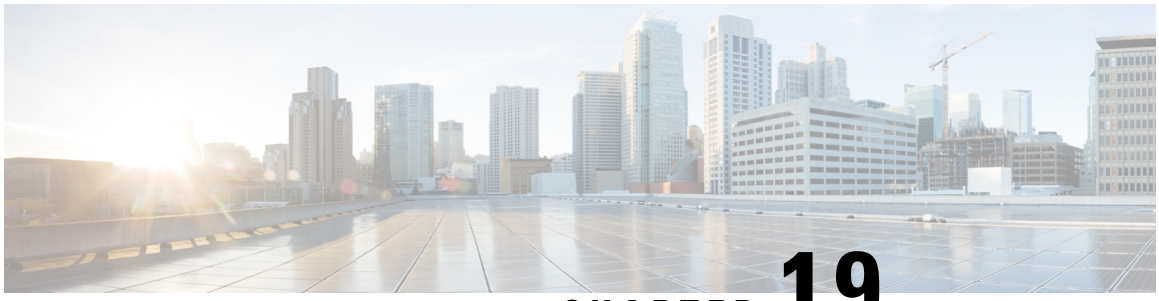


- Choose **Actions > Y.1564 Test** to test the performance of the CE circuit/VC end to end. See Running a Y.1564 Performance Test, on page 668.
- Choose **Actions > BERT** to test the performance of the Circuit Emulation Services. See Performance Test for Circuit Emulation Services, on page 673.
- Choose **Actions > Optical PM Parameters** to view the real time performance monitoring data of the optical circuit/VC. See Optical Performance Monitoring Parameters, on page 671.
- Choose **Actions > PRBS Test** to test the performance of the optical circuit/VC end to end. See Run PRBS Test on Circuits (ODU UNI), on page 672.
- Choose **Actions** > **Details** to view further details about the circuit. See Get Comprehensive Information About a Circuit/VC: Circuit/VC Details Window, on page 635.
- Choose **Actions** > **Restoration Actions** > **Upgrade Restore** to upgrade the failed optical circuit to an active route and delete the old route where the failure occurred. See Restore a Circuit (Optical), on page 645.
- Choose **Actions** > **Resync** to resync the conditions for the circuit or VCs.
- Choose **Actions** > **Restoration Actions** > **Manual Revert** to revert the optical circuit to its original route when the route is recovered from the failure. See Restore a Circuit (Optical), on page 645.
- Choose **Actions** > **Reroute Actions** > **Working Path** or **Protected Path** to reroute the traffic through the working path or protected path defined for the circuit. See Reroute a Circuit (Optical), on page 646.
- Choose **Actions** > **Activate** to allow the traffic to pass through the optical circuit. See Activate a Circuit (Optical), on page 644.
- Choose **Actions** > **Deactivate** to stop the traffic passing through the optical circuit. See Activate a Circuit (Optical), on page 644.
- Choose **Actions** > **Protection Actions**, and then choose the required protection switch action to switch over the traffic from one path to another path in a protected optical circuit. See Initiate a Protection Switch Action on a Circuit (Optical), on page 648

- Click the filter icon in the Multilayer Trace view toolbar to view the various layers in the circuit. Choose the layers that you want to be displayed.

PART VII

Administer the Cisco EPN Manager System



CHAPTER 19

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, on page 1.

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, on page 791.

Note Be sure to review the important information in Best Practices: Harden Your Cisco EPN Manager Security, on page 915.

Server Setup Tasks

Task	See
Verify the backup settings	Set Up Automatic Application Backups, on page 743
Install any required product licenses and software updates	Licenses and Software Updates, on page 697
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, on page 710

Task	See
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, on page 753
Configure high availability	Configure and Manage High Availability, on page 875
Adjust data retention and purging	Data Collection and Purging, on page 781
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, on page 777 Forward Alarms and Events as SNMP Trap Notifications, on page 846
Set up NTP (Network Time Protocol) so that time is synchronized between the server and network devices	Set Up NTP on the Server, on page 765
Configure FTP/TFTP on the server for file transfers between the server and network devices	Enable FTP/TFTP/SFTP Service on the Server, on page 767
Configure a proxy for the Cisco EPN Manager server	Set Up the Cisco EPN Manager Proxy Server , on page 766
Configure the email server	Set Up the SMTP E-Mail Server, on page 767
Enable the Compliance feature if you plan to use it to identify device configuration deviations	Enable and Disable Compliance Auditing, on page 152
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, on page 619
Configure product feedback to help Cisco improve its products	Set Up Defaults for Cisco Support Requests, on page 778

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, on page 765.
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, on page 589.

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, on page 597 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, on page 808 Disable and Enable the Web GUI root User, on page 792
Set up user authentication and authorization	Configure External Authentication, on page 823 Configure Local Authentication, on page 822
Create user accounts and user groups	Control the Tasks Web Interface Users Can Perform, on page 792

Task	See
Adjust user security settings (password rules for local authentication, idle time logout setting)	Configure Global Password Policies for Local Authentication, on page 813
Specify which users can approve jobs	Configure Job Approvers and Approve Jobs, on page 812
Create virtual domains to control device access	Create Virtual Domains to Control User Access to Devices, on page 815
Create a message that is displayed when users log in to the GUI client	Create a Login Banner (Login Disclaimer), on page 768

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, on page 846
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, on page 850
Customize the severity for specific events	Change Alarm Severity Levels, on page 853
Customize the auto-clear interval for specific alarms	Change Alarm Auto-Clear Intervals, on page 854
Make the text in the alarm **Failure Source** field more user-friendly	Change Alarm Severity Levels, on page 853
Customize the behavior of expedited events	Change the Behavior of Expedited Events, on page 856
Control generic event handling	Disable and Enable Generic Trap Processing, on page 860
Control if and how users can create Cisco Support Requests	Set Up Defaults for Cisco Support Requests, on page 778

Web GUI Setup Tasks (Admin)

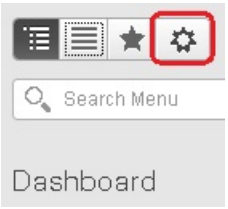
Task	See
Disable features or menu items that your deployment does not use	Customize the Web GUI Menus to Disable Cisco EPN Manager Features, on page 694
Set Up the System Monitoring Administration Dashboard	Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard, on page 772

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, on page 795. 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.

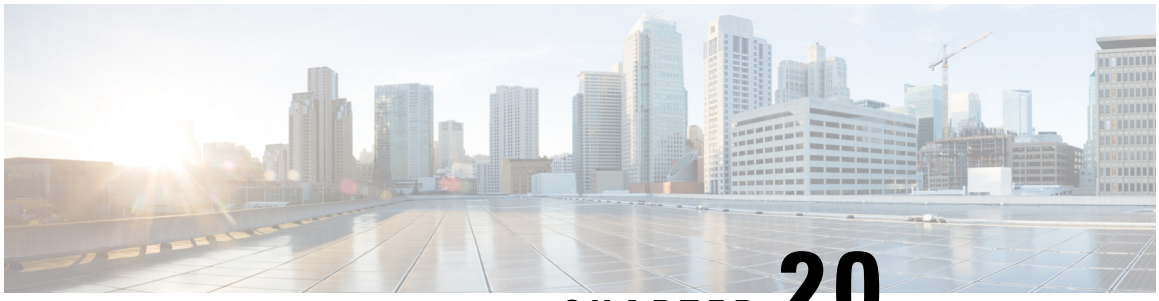
b. In the menu's **Status** column, click the toggle so that it displays **Disabled**. If you disable a menu that has sub-menus, the sub-menus are also disabled. For example:

- 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.



CHAPTER 20

Licenses and Software Updates

View and Manage Licenses

Licenses determine the features that you can use and the type and number of devices that Cisco EPN Manager can manage. When you connect to Cisco EPN Manager (without logging in), the login page displays a banner that identifies the type of license the server is running (see Types of Cisco EPN Manager Licenses, on page 697). If Cisco EPN Manager is configured to use single sign-on (SSO), check the license type by viewing the banner contents.

Cisco EPN Manager supports Cisco Smart Licensing and traditional licensing. If you are currently using traditional licensing, Cisco recommends that you convert to Smart Licensing. For information on the differences between the two types of licensing, refer to the Cisco Smart Licensing Overview on Cisco.com.

You can upgrade Cisco EPN Manager to a new version using one of the following licensing methods:

- Cisco Smart Licensing - In this method, you must register the new instance of the Cisco EPN Manager with the Cisco Smart Software Manager. See Register Cisco EPN Manager with the Cisco Smart Software Manager, on page 701.
- Traditional Licensing - In this method, the files are copied from the previous version of the Cisco EPN Manager to the upgraded version. However, you must purchase the Base license for the upgraded version. To purchase a new traditional license, go to http://cisco.com/go/license.

From Release 5.0, Smart license is enabled by default on all fresh installations of Cisco EPN Manager.

How to use Cisco Smart Licensing and traditional licensing is explained in the following topics:

- Use Cisco Smart Licensing, on page 699
- Use Traditional Licensing, on page 705

Types of Cisco EPN Manager Licenses

The following topics describe the feature and time-based licenses supported by Cisco EPN Manager.

Base License

A base license enables all applications and all device drivers (without device count restrictions) on the server. It is displayed in the web GUI as **Base License**.

Cisco Advantage Addon Function Right to Manage(RTM) License

The Cisco Advantage Addon Function RTM license is displayed in the web GUI as **Cisco Advantage Addon Function Right To Manage license**.

This license enables all features and options related to service discovery, provisioning, service promotion, service assurance, and multi-layer trace functions. Features and menu options related to these functions are not visible unless the license is active. Also, any scheduled provisioning jobs fail to run. After you install the first Cisco Advantage Addon Function Right to Manage (RTM) license, these features and options are enabled. Cisco EPN Manager licensing function tracks and reports use of this license in the licensing dashboard.

Device Right-to-Manage (RTM) License

Device RTM licenses allow the server to manage a specific number of devices of a specific device type. For RTM licenses, the device count is displayed next to the device type. These licenses come in two flavors:

- Extended RTM licenses for core, edge, aggregation, and access network devices. These licenses enable end-to-end network management: device lifecycle management, network provisioning, and network assurance.
- Foundation RTM licenses for service provider Wi-Fi networks that have Wi-Fi access points, WAN routers, core switches, and data center switches. Along with device lifecycle management, these licenses enable assurance visibility and troubleshooting capabilities.

Devices that are configured as satellites (for example, Cisco ASR 903 with a Cisco ASR 9000v host) are counted as independent devices.

Cisco EPN Manager also discovers third-party network devices. The collected information is displayed in the web GUI, but results can vary widely (depends on the responses Cisco EPN Manager receives from the devices).

RTM licenses are displayed in the GUI as follows:

- For Cisco devices—Device model, such as **NCS 2002** or **ASR 9001**.
- For third-party devices—Generic: Third Party Device.

SBY License for High Availability

The Standby (SBY) license allows the setup of high availability deployments. In a high availability deployment, all the device and feature licenses must be installed on the primary server. No licenses are required on the secondary server.

Time-Based, Lab, and Permanent Licenses

Most licenses can be purchased as a lab license or time-based license:

- Lab—For lab or staging environments.

  With lab license, there is no limit on the number of devices and types of devices you can manage. You can manage all devices in a staging environment with this license.

Note You can choose either the Lab license or the Device Right-to-Manage license to manage your devices. If you choose both the licenses, by default Cisco EPN Manager enables only the Lab license and automatically updates the license summary count of the Device Right-to-Manage license as zero.

- Time-Based (Evaluation)—For a 90-day trial period (the product is disabled when the trial period expires). If you purchase a time-based license, the days remaining are listed next to the license name.

These licenses can be converted to Permanent licenses.

Use Cisco Smart Licensing

Cisco recommends that you use the simple and efficient Cisco Smart Licensing mechanism to manage your licenses.

A comparison of Smart and traditional licensing is provided in the Cisco Smart Licensing Overview on Cisco.com. After enabling Smart Licensing in Cisco EPN Manager, you must register Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. After you are registered, all Cisco EPN Manager license types will be available to you from the Cisco EPN Manager web GUI.

If you are currently using traditional licensing, you can convert your existing Cisco EPN Manager licenses to Smart entitlements at any time, as described in Convert Traditional Licenses to Smart Entitlements, on page 703.

The following topics explain how to set up and manage Cisco EPN Manager licenses using Cisco Smart Licensing.

Set Up Cisco Smart Licensing in Cisco EPN Manager

Follow these steps to set up Cisco Smart Licensing so you can use it to manage your licenses. If you are currently using traditional licensing, use these same procedures to use Cisco Smart Licensing and, when convenient, convert your existing Cisco EPN Manager licenses as described in Convert Traditional Licenses to Smart Entitlements, on page 703.

	Step	See:
1.	Create a Smart Account with Cisco Systems.	Go to Smart Account Request and follow the instructions on the web site.

2.	Set up communication between Cisco EPN Manager and the CSSM on Cisco.com.	Set Up the Transport Mode Between Cisco EPN Manager and Cisco Smart Software Manager, on page 700
3.	Enable Smart Licensing in Cisco EPN Manager.	Enable Smart Licensing in Cisco EPN Manager, on page 701
4.	Register Cisco EPN Manager with the CSSM on Cisco.com by obtaining a token from the CSSM and entering it in the Cisco EPN Manager web GUI.	Register Cisco EPN Manager with the Cisco Smart Software Manager, on page 701
5.	Choose the licenses you want to use in Cisco EPN Manager.	Choose Cisco EPN Manager Licenses Using Smart Licensing, on page 702
6.	Set up the Smart License Dashboard so you can monitor your licensing usage.	Configure License Thresholds for the Smart License Dashboard, on page 703

Set Up the Transport Mode Between Cisco EPN Manager and Cisco Smart Software Manager

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Account Settings**.

Step 2 Click the **Smart Licensing Transport** tab and select a communication mode:

- Direct mode—Sends license information directly to the cloud. This is the default. You cannot edit this URL. Click **Test Connectivity** to check the connection status.
- Transport Gateway—Uses either a Cisco Smart Call Home transport gateway or a Cisco Smart Licensing Software satellite (which is installed at customer premises and provides a subset of CCSM functionality) for communication. (See Cisco.com for more details.) Enter the appropriate URL in the **Enter URL** field. Click **Test Connectivity** to check the connection status.
- HTTP/HTTPS Proxy—Uses either an HTTP or HTTPS proxy for communication between Cisco EPN Manager and the cloud. To enable this option, you must first configure the proxy settings. Click **HTTP/HTTPS Proxy** hyperlink or click the **Proxy** tab to add or edit the proxy settings. See Set Up the Cisco EPN Manager Proxy Server , on page 766.

Step 3 Click **Save** to save the transport settings.

Step 4 To revert to the default values, click **Reset**, and then click **Save**.

What to do next

If you have not already done so, enable Smart Licensing. See Enable Smart Licensing in Cisco EPN Manager, on page 701.

Enable Smart Licensing in Cisco EPN Manager

Before you begin

Make sure you have set up the transport mode. See Set Up the Transport Mode Between Cisco EPN Manager and Cisco Smart Software Manager, on page 700.

Step 1 Choose **Administration** > **Licenses and Software Updates** > **Smart Software Licensing**.

Step 2 Enable Cisco Smart Licensing in the Cisco EPN Manager web GUI.

a) Click the **Licensing Settings** tab.
b) In the **Licensing Mode** field, click **Smart Software Licensing** radio button.
c) Choose **Evolved Programmable Network Manager** from the Product Name drop-down list.
d) Click **Enable Smart Software Licensing**. Cisco EPN Manager may display a dialog box indicating that when you complete this procedure, you must restart the web GUI before you can proceed with the configuration step.
e) Click **OK** in the dialog box.
f) If necessary, log out of the web GUI and then log back in.

What to do next

Do one of the following:

- If you have not yet registered Cisco EPN Manager with the CSSM on Cisco.com, Cisco EPN Manager will run in evaluation mode (which has a limit of 90 days). Register the product as described in Register Cisco EPN Manager with the Cisco Smart Software Manager, on page 701.
- If you have registered Cisco EPN Manager with the CSSM, select the licenses you want to use. See Choose Cisco EPN Manager Licenses Using Smart Licensing, on page 702.

Register Cisco EPN Manager with the Cisco Smart Software Manager

To register Cisco EPN Manager with the CSSM, you must obtain a token from the CSSM and enter it into the Cisco EPN Manager web GUI. This is a one-time requirement. If for any reason you have to re-register your product instance, you can do that by following this procedure.

Note Refer to the Cisco Smart Software Manager User Guide for information on how to use the CSSM and the other actions that you can perform from this application—for example, renewing license registration and license authorization, unregistering the product from Cisco Smart Licensing, and so forth.

Before you begin

If your organization does not have a Smart Account, go to software.cisco.com, choose **Request a Smart Account** in the **Administration** area, and follow the instructions to create an account.

Step 1 Go to the Cisco Software Central web site (software.cisco.com).

Step 2 Obtain your tokens. If you already have tokens (for example, you converted traditional licensing PAKs to Smart entitlements), proceed to the next step.

If you are re-registering your product instance, your token will be listed in the CSSM user interface. If your token is no longer valid, you can obtain a new token using this procedure.

a. On Cisco Software Central, choose **License** > **Smart Software Licensing**.

b. Select the appropriate virtual account.

c. Click the **General** tab, then click **New Token**.

d. Follow the instructions to provide a name, duration, and export compliance applicability before accepting the terms and responsibilities.

e. Click **Create Token**.

f. Copy the Token ID to your clipboard and proceed to the next step.

Step 3 Enter the Token ID into the Cisco EPN Manager web GUI to register the product instance.

a. Choose **Administration** > **Licenses and Software Updates** > **Smart Software Licensing**.

b. Click the **Licensing Settings** tab, then paste your token into the **Registration Token** field.

c. Click **Register**.

Step 4 Log out of the Cisco EPN Manager web GUI, then log back in.

What to do next

Choose the licenses you want to use. See Choose Cisco EPN Manager Licenses Using Smart Licensing, on page 702.

Choose Cisco EPN Manager Licenses Using Smart Licensing

After you have registered Cisco EPN Manager with the CSSM, all Cisco EPN Manager license types will be listed in the Cisco EPN Manager web GUI, and you can choose the ones you want to use.

Step 1 If this is the first time you are choosing Smart licenses:

a) Choose **Administration** > **Licenses and Software Updates** > **Licenses**.

After a few moments, Cisco EPN Manager displays a dialog box informing you that you cannot access the page because you are not using traditional licensing. This is normal.

b) In the dialog box, click **Smart License Settings**.

c) Click the **Licensing Settings** tab.

Step 2 If you are already using Smart Licensing:

a) Choose **Administration** > **Licenses and Software Updates** > **Smart Software Licensing**.

b) Click the **Licensing Settings** tab.

Step 3 Under Smart License Usage, click **Choose Licenses**.

Step 4 Select licenses from the Available Licenses dialog box, then click **Save**. Cisco EPN Manager immediately begins consuming the licenses.

What to do next

Configure the Smart License Dashboard thresholds for the new licenses. See Configure License Thresholds for the Smart License Dashboard, on page 703.

Convert Traditional Licenses to Smart Entitlements

If you have been managing Cisco EPN Manager licenses using traditional licensing, you can enable and configure Smart Licensing by following the setup tasks in Set Up Cisco Smart Licensing in Cisco EPN Manager, on page 699. When convenient, convert your existing traditional licenses to Smart entitlements described in this procedure. You will have to enter your Product Activation Key (PAK) numbers in the License Registration Portal on the Cisco Software Central site.

Before you begin

- You must have a Cisco.com account to access Cisco Software Central. If you do not have an account, go to the Cisco Software Central.
- Make sure you have your existing traditional licensing PAK numbers.

Step 1 On Cisco Software Central, choose **License** > **Traditional Licensing**.

Step 2 Click **Continue to Product License Registration** to open the License Registration Portal.

Step 3 In the field under **Get New Licenses**, enter your PAK numbers. If you are entering multiple PAKs, separate them with a comma. You can enter a maximum of 10 PAKs.

Step 4 Under the **PAKs/Tokens** tab, select the PAKs you want to convert to Smart entitlements, then choose **Actions** > **Convert to Smart Entitlements**.

Configure License Thresholds for the Smart License Dashboard

To efficiently manage your licenses, configure the Smart License Dashboard to indicate when Cisco EPN Manager is approaching the point where its licenses will be depleted. The settings you configure here are system-wide .

Step 1 Choose **Administration** > **Licenses and Software Updates** > **Smart Software Licensing**, then click the **License Dashboard Settings** tab.

Step 2 Make a selection from the **License Type** drop-down list.

Step 3 Enter a value in the **Threshold Value** field.

Step 4 Click **Save**.

The threshold value is displayed as a straight line in the graphical representation of the **License Summary** and the **Device Distribution for License** dashlets.

Check Cisco EPN Manager License Usage

Check current license usage using the Smart Licensing Dashboard. To open the dashboard, choose **Administration** > **Dashboards** > **Smart Licensing Dashboard**. For an explanation of the basic license types, see Types of Cisco EPN Manager Licenses, on page 697.

To view these license counts:	Check this part of the dashboard:
For the current date	License Summary Count—Green indicates compliant license counts; red indicates non-compliant license counts.
For a specific week or month	License Summary—Hover over a bar chart to view more details.
For a specific license type	Device Distribution for License—Click one of the license links at the top of the License Summary dashlet. Hover your mouse cursor over the chart to view the details.

Disable Smart Licensing

Step 1 Change the license setting in the Cisco EPN Manager web GUI.

a) Choose **Administration** > **Licenses and Software Updates** > **Smart Software Licensing**.

b) At the bottom of the page, click **Disable Smart Licensing**, then confirm your choice.

Step 2 Log out of the Cisco EPN Manager web GUI, then log back in.

Because Cisco EPN Manager is not yet registered to use traditional licensing, when you log back in, all features are disabled. This is normal.

Step 3 Enable traditional licensing in the Cisco EPN Manager web GUI. (This is done from the Smart License Settings page.)

a) Choose **Administration** > **Licenses and Software Updates** > **Licenses**.

After a few moments, Cisco EPN Manager displays a dialog box informing you that you cannot access the page because you are not using traditional licenses. This is normal.

b) In the dialog box, click **Smart License Settings**.

c) Click the **License Settings** tab.

d) For the Licensing Mode, select **Traditional Licensing**.

e) Click **Register**.

Step 4 Log out of Cisco EPN Manager, then log back in.

Reference: Smart Product Registration and License Authorization Statuses

Product Registration Status

The License Registration Status reflects whether the product is properly registered with Cisco Smart Software Licensing on Cisco.com.

License Registration Status	Description
Unregistered	Smart Software Licensing is enabled in Cisco EPN Manager but Cisco EPN Manager is not registered with the CSSM.
Registered	Cisco EPN Manager is registered with the CSSM. Cisco EPN Manager has received an ID certificate that will be used for future communication with the Cisco licensing authority.
Registration Expired	Cisco EPN Manager did not successfully renew its registration prior to the expiration date and has been removed from CSSM.

License Authorization Status

The License Authorization status reflects license usage against purchased licenses, and whether you are in compliance with Cisco Smart Licensing. If you exceed the number of purchased licenses, the product's status will be **Out of Compliance**.

License Authorization Status	Description
Evaluation Mode	Cisco EPN Manager is running in evaluation mode (expires in 90 days).
Authorized	Cisco EPN Manager has a valid Smart Account and is registered. All licenses requested by the product are authorized for use.
Out of Compliance	Cisco EPN Manager has exceeded the number of licenses that were purchased. (Specifically, the virtual account for the product instance has a shortage of one or more licenses types.)
Evaluation Expired	The evaluation period has expired and Cisco EPN Manager is in the unlicensed state.
Authorization Expired	Cisco EPN Manager did not successfully renew its license authorization prior to the authorization expiration date.

Use Traditional Licensing

Note Cisco recommends that you convert to Cisco Smart Licensing. See Set Up Cisco Smart Licensing in Cisco EPN Manager, on page 699. If you are using Smart Licensing and want to re-enable traditional licensing, see Disable Smart Licensing, on page 704.

Cisco EPN Manager checks traditional licenses every 4 hours and writes the status to the License log (/opt/CSCOlumos/logs/license.log). If a time-based license expires, any users that are in an active session will be redirected to the **Licenses** page, and new users are prevented from logging in. If an RTM license device count is exceeded, you should either:

- Delete some of the devices. After the daily inventory collection, the devices will be displayed as **Managed**.

- Obtain a license with a higher RTM count. See Add and Delete Traditional Licenses, on page 706.

See these topics for more information on traditional licenses:

- Types of Cisco EPN Manager Licenses, on page 697
- View Traditional Licenses, on page 706
- Add and Delete Traditional Licenses, on page 706
- Move a Traditional License to Another Server, on page 706

View Traditional Licenses

To view the traditional Cisco EPN Manager licenses that are currently installed, choose **Administration** > **Licenses and Software Updates** > **Licenses**. Cisco EPN Manager supports the licenses listed under **Base License**.

Note A separate license is used by each chassis in a multi shelf device. For example, if a Cisco NCS 2006 device houses 3 chassis, 3 licenses are used by that device.

Add and Delete Traditional Licenses

To install a new traditional license, the original license must already reside on the server. Do not create copies of licenses. To purchase new traditional licenses, go to www.cisco.com/go/license. Make sure you install licenses in the correct order. For example, you must always install the Base license first because it is required by the other licenses.

When you delete a license, all of that license's information is removed from the server.

Caution If you make a manual change to a license file, Cisco EPN Manager considers the file corrupted and will not install it. If this happens, obtain a new license file.

Step 1 Choose **Administration** > **Licenses and Software Updates** > **Licenses**.

Step 2 Choose **Files** > **License Files**.

- To add a license, click **Add**, click **Choose File**, browse to the location of the license file, and then click **OK**.
- To delete a license, select the license file, then click **Delete**.

Move a Traditional License to Another Server

The only time you may have to move a license to another server is if you are using high availability, and a server fails. If you need to delete a license, see Add and Delete Traditional Licenses, on page 706. To move the license:

Step 1 Delete the traditional licenses from the original server.

Step 2 Send an e-mail to licensing@cisco.com requesting a *re-host* for your traditional licenses.

Step 3 When you receive the traditional license, install it on the new server.

Renewing an Expired License

If your Cisco EPN Manager license has expired, you can complete the following procedure to renew it:

Step 1 Choose **Administration** > **Licenses and Software Updates** > **Licenses**.

The **Licenses** page opens.

Step 2 Do one of the following:

- If you see the **Summary** and **Files** menus in the top left portion of the page, skip ahead to Step 4.
- If you do not see these menus, you will first need to register traditional licensing. Proceed to Step 3.

Step 3 Register traditional licensing, then return to Step 1 of this procedure:

a) Choose **Administration** > **Licenses and Software Updates** > **Smart Software Licensing**.
b) With the **Licensing Settings** tab selected, click the **Traditional Licensing** radio button, then click **Register**.
c) Log out of Cisco EPN Manager, then log back in.

Step 4 From the top left area of the page, choose **Files** > **License Files**.

The **License Files** page opens.

Step 5 Choose the license file you want to renew:

a) Click **Add**.

The **Add A License File** dialog box opens.

b) From the **Select License File** field, click **Choose File**.
c) Navigate to and click the appropriate license file, then click **Open**.
d) Click **OK**.

Step 6 Log out of Cisco EPN Manager, then log back in.

View the Licensing Dashboard

From the **Licensing** dashboard, you can determine whether traditional or smart software licensing is enabled (indicated in the **Active Licensing Mode** field at the top of the dashboard) and view the number of licenses that are currently in use. You can set the licensing mode from the **Smart Software Licensing** page (**Administration** > **Licenses and Software Updates** > **Smart Software Licensing**).

To open the dashboard, do one of the following:

- Choose **Administration** > **Dashboards** > **Licensing Dashboard**.
- Click the **Licensing Dashboard** link from the top-right corner of the **Smart Software Licensing** page.

The information displayed in the dashboard depends on the licensing mode that is enabled. If smart software licensing is currently enabled, the following dashlets are displayed:

- **License Summary Count** area—Displays the number of licenses consumed and the compliance status for each license type. The number of licenses displayed is based on the current date.
- **License Summary** dashlet—Displays a bar chart that graphs the number of licenses consumed for each license type during a particular time period. To view additional information, place your cursor over the chart.
- **Device Distribution for License** dashlet—To view the device distribution chart for a particular license, click its link from the top of the chart displayed in the **License Summary** dashlet. To view additional information, place your cursor over the chart.

Note The information displayed in the **License Dashboard** is refreshed daily after the SmartLicense job runs at 02:00 a.m. (its pre-configured run time). To view this job in the **Job Dashboard**, choose **Administration** > **Dashboards** > **Job Dashboard**.

If traditional licensing is currently enabled, the **Licensing** dashboard displays the **Traditional Licensing** dashlet. Specify whether you want to view information about Small, Medium, Large, or Generic licenses by choosing the corresponding option from the **License Type** drop-down list. The dashlet updates, displaying information such as the device families with that license type, the number of tokens allocated to each device in those families, as well as the number of tokens that are not being used at the moment.

Related Topics

Set Up Cisco Smart Licensing in Cisco EPN Manager, on page 699
Enable Smart Licensing in Cisco EPN Manager, on page 701
Register Cisco EPN Manager with the Cisco Smart Software Manager, on page 701
Configure License Thresholds for the Smart License Dashboard, on page 703
Disable Smart Licensing, on page 704
Reference: Smart Product Registration and License Authorization Statuses, on page 704

Manage Software Updates

What Are Software Updates?

Cisco provides updates to the Cisco EPN Manager software periodically. These updates fall into the following three categories:

- Critical Fixes—Provide critical fixes to the software. We strongly recommend that you download and apply all of these updates as soon as they are available.
- Device Support—Adds support for managing devices which Cisco EPN Manager did not support at release time.

- Add-ons—Provide new features, which can include GUI screens and functionality, to supplement the Cisco EPN Manager version you are using. This includes Cisco EPN Manager maintenance packs and maintenance pack point patches.

The update notifications that Cisco EPN Manager displays depend on the Notification Settings specified by your administrator. See Enable or Disable Notifications About Software Updates, on page 710 . All software updates are packaged in .ubf files. A large update can contain individual smaller updates, from which you can choose what you want to install. When you install an update, Cisco EPN Manager does the following:

- Verifies that the file publisher is Cisco Systems and the file has not been tampered with.
- Automatically installs any other updates that are required.

If you have connectivity to http://www.cisco.com , you can download and install the updates directly from Cisco.com. If you do not have internet connectivity, copy the update from a server that has the necessary connectivity and install it from there.

See the Cisco EPN Manager Installation Guide for installation instructions for maintenance packs. For point patch installation instructions, see the readme file provided with the patch file on the Software Download page on Cisco.com.

View the Installed Product Software Version

Use one of these methods to check the Cisco EPN Manager product version:

- From the Web GUI, click the Settings icon at the top right of the page, and choose **Help** > **About Cisco EPN Manager**.
- From the CLI, view the contents of the file named

  #cat /opt/CSCOlumos/installedComponentsVersions.xml

To use the CLI, see Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

View Installed Software Updates

If you are not logged in to the web GUI, you can view a pop-up window that lists the software updates by clicking **View Installed Updates** from the login page.

If you are logged in to the web GUI, you can view the software updates in two ways:

- From the **About Cisco EPN Manager** page, by clicking the settings icon at the top right of the page and clicking **About Cisco EPN Manager**, and then clicking **View Installed Updates**. (The **View Installed Updates** link is also available from the login page.)
- By choosing **Administration** > **Licenses and Software Updates** > **Software Update** (this method provides the most detail).

The **Software Update** page displays two tabs:

- **Installed Updates**—Updates that Cisco EPN Manager is currently using.
- **Uploaded Update Files**—Update files that have been uploaded to the server (including those that are not being used). The Corresponding Updates field lists any prerequisite updates that were also uploaded.

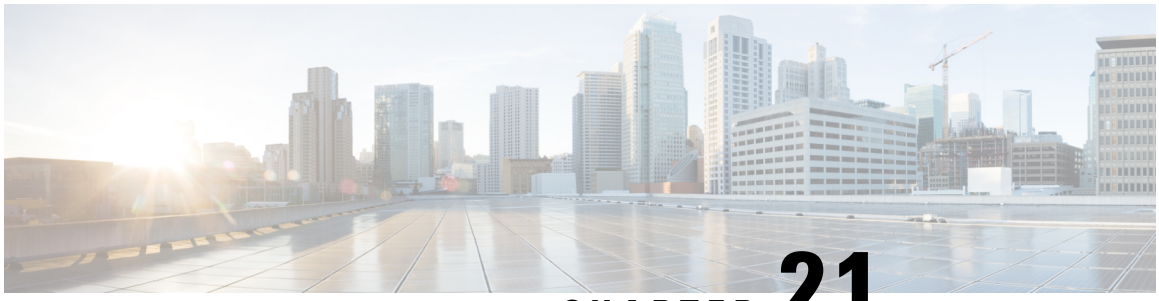
  If an update file has not yet been installed, it can be deleted. Select the file and click the **Delete** button.

Enable or Disable Notifications About Software Updates

By default, Cisco EPN Manager displays information about all available updates in the **Software Updates** page. Because the list can be quite long, you may want to adjust what is displayed and the updates for which you are notified. You can also disable all notifications and re-enable them later.

Configure your software update notification settings.

a) Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Software Update**.
b) Under **Notification Settings**, select or deselect the update categories. To disable all notifications, make sure no categories are selected. For an explanation of the categories, see What Are Software Updates?, on page 708
c) Click **Save**.



CHAPTER 21

Cisco Evolved Programmable Network Manager Security

This chapter consists of the following topics:

Security Overview

Cisco EPN Manager requires a high level of security to ensure that your network and its data are not compromised. This is especially important because it has full management control over your network and stores device credentials. To this end, Cisco EPN Manager leverages the following security approaches:

- **Secure architecture**: The Cisco EPN Manager architecture is designed to limit access to any unknown software flaws that may be present so they cannot be used for a malicious purpose.
- **Secure default configurations**: Cisco EPN Manager is shipped with a default configuration that enhances the security of the product. For example, even though insecure FTP and TFTP services are supported, they are not activated in the default configuration.
- **Installation hardening**: Cisco's Advanced Services team can evaluate the specifics of your Cisco EPN Manager installation and complete the additional security hardening tasks that may be needed.
- **Cisco Secure Development Lifecycle (CSDL) process**: From development to release, the CSDL process is followed to improve security of Cisco EPN Manager.
- **Two-factor Authentication**: Users must go through two layers of security before being granted access to Cisco EPN Manager.

The following sections describe these approaches in more detail.

Secure Architecture

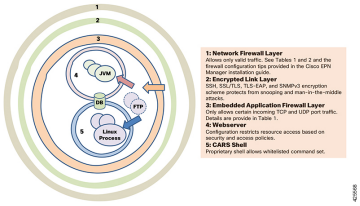
Cisco EPN Manager's architecture design is based on the premise that 3 conditions must exist simultaneously in order for an attacker to breach a system:

- The system has a flaw.
- The attacker has access to that flaw.
- The attacker is capable of exploiting the flaw for a malicious purpose. (Hughes, J., & Cybenko, G. 2013. Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. *Technology Innovation Management Review*, 3(8): 15-24.)

On its own, a flaw is benign. It is only when an attacker can access the flaw and knows how to exploit it that the flaw becomes a vulnerability. This distinction between a flaw and a vulnerability is important to understand. Just because a flaw has gone public does not automatically mean it has become a vulnerability. And a flaw may only be a vulnerability under certain circumstances.

Limiting access to system flaws is key to the approach Cisco EPN Manager uses to manage security risks. We have designed the Cisco EPN Manager architecture so that any flaws that may be found should not be readily accessible to an attacker. This is a practical and reasonable approach because you cannot always eliminate flaws or prevent an attacker from exploiting them. What you can do is limit access to certain flaws that exist by putting multiple layers of security in place. Cisco EPN Manager uses three layers of perimeter security, as illustrated in Figure 1.

Figure 16: Multilayer Secured Perimeter Architecture: A Virtual Appliance System with Hardened Exterior Shell



Of these three layers, one resides within and two reside outside of Cisco EPN Manager. The interior layer is preconfigured with Cisco EPN Manager and becomes operational after the installation is completed. The two exterior layers are not preconfigured and need to be implemented by creating an exterior network firewall and encrypted communication link layer. We recommend that your company's technical team works with Cisco Advanced Services to create these items.

Note You may need to modify some configurations within Cisco EPN Manager in order to choose the right kind of encryption protocols to use for your network.

The interior layer is built into Cisco EPN Manager and consists of the following components:

- Embedded firewall—Provides the first protective layer around the interior components. This allows only a few ports to be open to incoming traffic. This decreases the attack surface by limiting access to multiple flaws (both known and unknown) in the Linux OS and Oracle databases.
- CARS shell—Provides a protective layer around Linux by enforcing an approved list of allowed commands that can be run on Linux, thus restricting interaction with the OS.

- Web server—Provides a protective layer around Linux, the Java virtual machine, and the database. This layer has security filters in place for restricting access to Java as well as the database resources and methods.

This interior layer protects the system against many risks, such as the ones described in the following examples. While these flaws are deemed vulnerabilities in an unprotected system, these are not in Cisco EPN Manager. In these examples (identified by their National Vulnerability Database ID), we will assume that the external firewall and encrypted links layer have either been breached by an attacker or are non-existent:

- CVE-2013-5211: Flaw in NTP's implementation of the Linux NTPD component—A DoS attack takes place after incoming NTP traffic is accessed from port 23. Since the embedded firewall disallows this traffic, this flaw is not accessible to an attacker and therefore not a risk in Cisco EPN Manager.
- CVE-2016-0634: Linux bash shell flaw—This attack can be made by an authenticated user that has targeted a bash shell through port 22. Cisco EPN Manager does not offer direct access to a bash shell via port 22. Instead, a CARS shell is accessible by regular authenticated users. As a result, this flaw is not a risk in Cisco EPN Manager.
- CVE-2017-12617: Apache Tomcat flaw—This attack can happen when a PUT request is made. Since Cisco EPN Manager's webserver configuration does not allow this kind of access, this flaw is not a risk.
- CVE-2015-4863: Oracle database flaw—This attack can happen on a network via the Oracle Net protocol. This flaw is not a risk in Cisco EPN Manager since the Oracle database resides behind the built-in firewall and webserver. As a result, it is not possible to access the database over the network.

Implications of the Security Architecture

Due to this architecture, Cisco EPN Manager is a very tightly integrated system, with an embedded OS and database that are not open to user access for any management or operations purposes. Users can only access and manage the system using Cisco EPN Manager GUI and Cisco EPN Manager Admin CLI. This Admin CLI is not a Linux CLI (see User Interfaces and User Types, on page 789). In addition, Cisco EPN Manager is deployed and managed as a virtual appliance, meaning Cisco EPN Manager is available as a OVA file to be deployed as standalone virtual machine (VM). Hence, management of Cisco EPN Manager is very different from managing a web application running on top of Linux OS and connected to a database. This means, users:

- Cannot patch/upgrade individual components by third-party/non-Cisco patches. Cisco will release patches for all internal components, including embedded Linux and Oracle.
- Cannot install third-party applications on embedded Red Hat Linux OS, for any purpose, as Cisco cannot provide technical support.
- Cannot readily manage embedded components - Linux, Oracle, Java, like a regular server.
- Should not try to change any internal configuration that are not mentioned as user modifiable in this guide, because such changes can either weaken the overall security, or disable/degrade the functionality or performance of the system.

Note Cisco EPN Manager is not a regular web application running on Linux OS and connected Oracle database, even though it has embedded Linux and Oracle underneath. In other words, the sum of the total is not same as the sum of the parts.

Cisco EPN Manager is a tightly integrated virtual appliance with hardened exterior shell. This means that the criteria used to evaluate security of Linux, Oracle, and regular web applications can NOT be used to evaluate Cisco EPN Manager. One cannot use the criteria of Linux OS for evaluating Oracle, as those are different products. Similarly, one cannot use the criteria and methods meant for Linux to evaluate Cisco EPN Manager or the ones that are for Oracle to judge Cisco EPN Manager. To evaluate Cisco EPN Manager security, one needs a different set of criteria and test methods that are suitable for Cisco EPN Manager architecture.

Ports Used by Cisco EPN Manager

Cisco EPN Manager ships with a built-in application firewall configuration to ensure that only legitimate traffic is allowed into the server. Table 1 lists the ports used to listen for connection requests from devices and accept incoming traffic. The opening and closing of these ports in the firewall is done automatically by Cisco EPN Manager when you enable or disable certain features. There is no need to enable or disable the ports within the firewall. If you try to specify any firewall configurations that circumvent Cisco EPN Manager, you may compromise its security and integrity.

Note The following table also provides information required to carry out post-installation security hardening (see Secure Default Configurations for more information).

Table 54: Listening Ports That Are Open Through Built-in Firewall

Port	Protocol	Usage	Safe to Disable?	Notes
21	TCP	To transfer files to and from devices using FTP.	Depends	This might be still needed by older managed devices that only support TFTP and not SFTP or SCP. Method to disable this port - Disable FTP from the web GUI under **Administration > Settings > System Settings**, then choose **General > Server**. After disabling FTP, as the CLI admin user, stop and restart the server.
22	TCP	To initiate SSH connections with the Cisco EPN Manager server, and to copy files to the Cisco EPN Manager server using SCP or SFTP.	No	—

Port	Protocol	Usage	Safe to Disable?	Notes
69	UDP	To distribute images to devices using TFTP.	Depends	Only if alternative protocols like SCP or SFTP or HTTPS are used for image distribution, and if supported by the managed devices.
162	UDP	To receive SNMP traps from network devices.	No	—
443	TCP	For browser access to the Cisco EPN Manager server via HTTPS.	No	—
514	UDP	To receive syslog messages from network devices.	No	—
1522	TCP	For High Availability (HA) communication between active and standby Cisco EPN Manager servers. Used to allow Oracle JDBC traffic for Oracle database synchronization.	Yes	If at least one Cisco EPN Manager server is not configured for HA, this port is automatically disabled.
2021	TCP	To distribute images to devices using FTP.	No	—
6789	TCP	Used for Java Remote Method Invocation (RMI) operations.	Yes	—
8005	TCP	Tomcat shutdown server socket port	Yes	—
8082	TCP	For the HA Health Monitor web interface (via HTTPS). Used by primary and secondary servers to monitor their health status via HTTPS.	No (If HA configured)	—
8085	TCP	Used by the Health Monitor process to check network bandwidth speed between primary and secondary servers, when the user executes readiness test under high availability.	No (If HA configured)	—
8087	TCP	To update software on the HA secondary backup server (uses HTTPS as transport).	No	—
8091	TCP	This port is used by the Web Container.	Yes	—
8456	TCP	It is used by Tomcat HTTP connector for HTTP/1.1 requests.	Yes	—

Port	Protocol	Usage	Safe to Disable?	Notes
8457	TCP	This port acts as a connector port to handle SSL requests since HTTP connector cannot handle SSL requests.	Yes	—
9991	UDP	To receive Netflow data packets.	Yes	Cisco EPN Manager does not support Netflow. You should disable this traffic in the network firewall.
9992	TCP	To manage M-Lync using HTTP or HTTPS.	Yes	Cisco EPN Manager does not support M-Lync. You should disable this traffic in the network firewall.
11011 to 11014	TCP	For PnP operations for proprietary Cisco Network Service (CNS) protocol traffic.	Yes	Cisco EPN Manager does not support PnP. You should disable this traffic in the network firewall.
61617	TCP	For MTOSI NBI notification over Java Message Service (JMS) connections. Also used for PnP operations.	Yes	Cisco EPN Manager does not support MTOSI over JMS or PnP. You should disable this traffic in the network firewall.

Secure Default Configurations

Cisco EPN Manager ships with default application configurations that are as secure as possible. You should only modify them after you have analyzed the threat model and assessed the risks for your specific situation. With the default configurations, Cisco EPN Manager does its best to:

- Not use default passwords.
- Not make unnecessary OS and Oracle packages/services accessible.
- At the time of a Cisco EPN Manager release, the latest security patches are applied for the embedded OS and Oracle.
- Not allow the use of Oracle access passwords by human users. These passwords are machine-generated and used by internal components.

Harden Your Installation

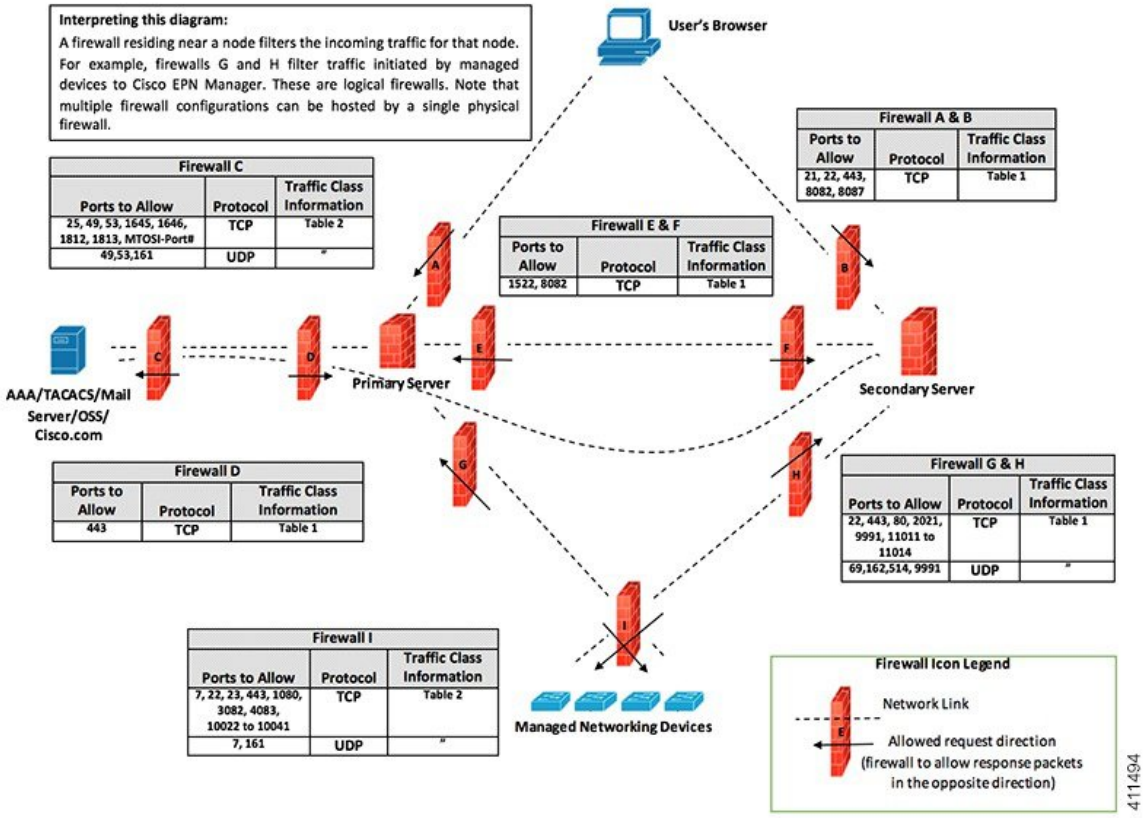
To harden your Cisco EPN Manager installation, you need to complete the following tasks:

1. Configure the built-in interior and exterior network firewalls to allow only legitimate traffic.
2. Use encryption for all incoming and outgoing traffic.

3. Configure Cisco EPN Manager and its peer systems to allow the transmission of only legitimate transactions.

Before you proceed, you should first understand how Cisco EPN Manager interacts with peer systems. This, along with management traffic flows and the exterior network firewalls for a generic HA deployment, is illustrated in the following figure.

Note Although we recommend that you implement these firewalls, you are not required to do so.



Depending on your installation, you may need to customize the firewall configuration to further improve security. As a general policy, any ports that are not needed and not secure (i.e. do not transmit encrypted traffic) should be disabled.

Configure the Built-In Application Firewall

To configure the application firewall, you need to disable the Cisco EPN Manager features that your installation does not need to run. This will automatically shut down the corresponding listening ports in the firewall.

Step 1 Identify the ports that are currently enabled:

a) To view a list of the ports used in your deployment that are exposed externally, log in as a Cisco EPN Manager CLI admin user and then run the **show security-status** command.

b) To view a list of all open listening ports at the OS level, log in as the CLI admin user and then run the **show netstat** command.

Step 2 Using Table 54: Listening Ports That Are Open Through Built-in Firewall , on page 714 for guidance, determine which of these ports can be safely disabled without disrupting the normal functioning of Cisco EPN Manager.

Note the following:

- Cisco EPN Manager uses some of the listening ports for its internal operations. These ports are kept hidden behind the built-in firewall.
- You should only use the procedure provided in Table 54: Listening Ports That Are Open Through Built-in Firewall , on page 714 to enable or disable ports.

Set Up Exterior Network Firewalls

In addition to the built-in firewall, you can also deploy network firewalls that only allow traffic targeted at the listening ports used by Cisco EPN Manager and its peer systems. The figure provided in the Harden Your Installation topic illustrates how the port information listed in Table 54: Listening Ports That Are Open Through Built-in Firewall , on page 714 and Table 55: Destination Ports Used by Cisco EPN Manager, on page 718 are used to set up firewall rules. Use this figure to decide on the appropriate firewall configurations for your management network.

- To identify the traffic class, refer to the **Usage** column in Table 54: Listening Ports That Are Open Through Built-in Firewall , on page 714. We recommend that you disable the ports used by the services that are not used by your Cisco EPN Manager installation.
- You should also enable the destination ports that Cisco EPN Manager uses for outgoing traffic (to connect to network devices or peer systems) in your network firewalls. Refer to Table 55: Destination Ports Used by Cisco EPN Manager, on page 718 for a listing of these destination ports and their purpose.

Table 55: Destination Ports Used by Cisco EPN Manager

Port	Protocol	Used to:
7	TCP/UDP	Discover endpoints using ICMP.
22	TCP	Initiate SSH connections with managed devices.
23	TCP	Communicate with managed devices using Telnet.
25	TCP	Send email using an SMTP server.
49	TCP/UDP	Authenticate Cisco EPN Manager users using TACACS.
53	TCP/UDP	Connect to DNS service.
161	UDP	Poll using SNMP.
443	TCP	Upload or download images and perform configuration backup-restore for Cisco NCS 2000 devices using HTTPS.

Port	Protocol	Used to:
1522	TCP	Communicate between primary and secondary HA servers (allows Oracle JDBC traffic for Oracle database synchronization between primary and secondary servers).
1080	TCP	Communicate with Cisco Optical Networking System (ONS) and Cisco NCS 2000 series devices using Socket Secure (SOCKS) protocol.
1645, 1646, and 1812, 1813	UDP	Authenticate Cisco EPN Manager users using RADIUS.
3082	TCP	Communicate with Cisco ONS and Cisco NCS 2000 devices using TL1 protocol.
4083	TCP	Communicate with Cisco ONS and Cisco NCS 2000 series devices using TL1 protocol.
8082	TCP	Communicate between primary and secondary HA servers to monitor each other's health using HTTPS.
8085	TCP	Used by the Health Monitor process to check network bandwidth speed between primary and secondary servers, when the user executes readiness test under high availability.
10022 to 10041	TCP	Passive FTP file transfers (for example, device configurations and report retrievals).
MTOSI/RESTCONF TCP port number	TCP	Listen at NBI client connected to the Cisco EPN Manager server (after this port is configured by NBI client system, a registration notification message containing the port number is sent to Cisco EPN Manager server); refer to the MTOSI or RESTCONF API guide for more information.

Set Up Traffic Encryption

You will need to encrypt the following traffic groups:

- Northbound traffic—This group consists of either client-server traffic from a human user's browser or NBI traffic from a Business Support System/Operational Support System (BSS/OSS). This traffic is transmitted over HTTP, so you need to implement HTTPS (HTTP encrypted by TLS).
- Southbound traffic—This group consists of management traffic that queries or configures managed devices using a wide range of protocols such as SNMP and HTTP. Protocols such as SSH and SNMPv3 may be used to secure this traffic. For a description of the configuration steps that need to be completed in order to encrypt this traffic, see Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices.
- East-West traffic between peer systems—This group consists of traffic between Cisco EPN Manager and a variety of other supporting systems like an external authentication server (secured by TLS-EAP) or a SMTP mail server (secured by TLS). Different encryption protocols are used, depending on the application protocol that needs to be protected. Some of the application protocols may also have built-in encryption.

- East-West traffic between a primary and secondary server in an HA deployment—This group consists of traffic between two Cisco EPN Manager servers running in primary and secondary mode. Each server monitors the other's health and keeps database and other file content synchronized over a connection secured by HTTPS.

Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices

SNMPv3 is a higher security protocol than SNMPv2. If your devices support SNMPv3, configure the devices to use SNMPv3 to communicate with the Cisco EPN Manager server. The following procedures explain how to specify SNMPv3 when adding new devices.

Method for Adding Devices	How to Specify SNMPv3	For more information, see:
Add a single device	In the **Add Device** dialog box, go to the **SNMP Properties** page and choose **v3** from the **Versions** drop-down list.	Add Devices Manually (New Device Type or Series), on page 44
Add multiple devices (bulk import)	When you edit your CSV file, enter the following: • Enter **3** in the **SNMP Version** column. • Enter the appropriate values for these columns: **snmpv3_user_name**, **snmpv3_auth_type**, **snmpv3_auth_password**, **snmpv3_privacy_type**, and **snmpv3_privacy_password**	Import Devices Using a CSV File, on page 42
Add multiple devices using discovery	In the **Discovery Settings** dialog box, go to the **Credential Settings** area and click **SNMPv3 Credentials**. Click the + sign to add the device credentials.	Run Discovery with Customized Discovery Settings, on page 40

Before you begin

Make sure SNMPv3 is enabled (with the appropriate security algorithm, such as HMAC-SHA-96) on the network devices that support it.

Set Up External Authentication Using the CLI

We recommend that you manage user accounts and passwords using a dedicated, remote authentication server running a secure authentication protocol such as RADIUS or TACACS+. In addition to setting up authentication using the following procedure, contact your external authentication vendor for additional security hardening suggestions.

Note If you decide to use local user authentication, check the default password policies to determine whether you want to make them stronger. See Configure Global Password Policies for Local Authentication, on page 813.

Configure Cisco EPN Manager to authenticate users using an external AAA server. You can configure the server using the web GUI or by using the command line interface (CLI). To set up remote user authentication via the GUI, see Configure External Authentication, on page 823.

To configure external authentication using the CLI, follow these steps. EPNM supports configuring only TACACS+ via CLI

Step 1 Log in to Cisco EPN Manager using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter config mode.

Step 3 Enter the following command to setup an external authentication TACACS+ server:

```
aaa authentication tacacs+ server tacacsIP key plain shared-secret
```

Where:

- *tacacsIP* is the IP address of an active TACACS+ server.
- *shared-secret* is the plain-text shared secret for the active TACACS+ server.

Step 4 Enter the following command to create a user with administrator privileges, who will be authenticated by the server specified in the previous step:

```
username username password remote role admin [email emailID]
```

Where:

- *username* is the name of the user ID.
- *password* is the plain-text password for the user.
- *emailID* is the email address of the user (optional).

Harden SSH Against Brute-Force Password Attacks

Since password-based SSH authentication is vulnerable to brute-force attacks, we recommend that you switch to one of the accepted Public Key types (PubkeyAcceptedKeyTypes) after installing Cisco EPN Manager. The list of accepted Public Key type (PubkeyAcceptedKeyTypes) in the Cisco EPN Manager are:

- ecdsa-sha2-nistp256-cert-v01@openssh.com
- ecdsa-sha2-nistp384-cert-v01@openssh.com
- ecdsa-sha2-nistp521-cert-v01@openssh.com
- ssh-ed25519-cert-v01@openssh.com
- ssh-rsa-cert-v01@openssh.com
- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384

- ecdsa-sha2-nistp521
- ssh-ed25519

To make the switch, follow these steps:

Step 1 Log in as the Linux CLI admin user and access the shell.

Step 2 Check who the current user is:

```
# whoami
```

The resulting output should indicate that you are the Linux admin user, not the Linux root user.

Step 3 For the Cisco EPN Manager admin user, use one of the accepted Public Key types (PubkeyAcceptedKeyTypes) to create key pairs and an SSH string using a tool (such as puTTYgen) with at least 2048-bit strength.

For example, generate a key using ed25519 like this:

```
$ ssh-keygen -t ed25519 -N ""
```

The SSH string should look something like this:

```
ssh-ed25519 AAAAC3Nza... ......root@localhost.localdomain
```

Tip Save the private key in a file, preferably in encrypted form with a passphrase. Also keep the passphrase handy.

Step 4 Create the authorized_keys file and assign the appropriate access privileges to the Cisco EPN Manager admin user:

a) In the admin user's home directory, create the .ssh directory and assign read, write, and execute privileges for this directory to only the admin user:

```
# cd ~
# mkdir .ssh
# chmod 700 ~/.ssh
```

b) Create the authorized keys file:

```
# cd .ssh
# vi authorized_keys
```

c) Copy and paste the SSH string you created in Step 3 in to the authorized_keys file and then save the file.

d) Assign read, write, and execute privileges for the authorized_keys file to only the admin user:

```
# chmod go= ~/.ssh/authorized_keys
# chmod u=rwx ~/.ssh/authorized_keys
```

e) Confirm you assigned the appropriate access privileges to the authorized_keys file:

```
# ls -al
```

The resulting output should look something like this:

```
total 6
drwx------. 2 admin gadmin 1024 May 10 00:25 .
drwx------. 6 admin gadmin 1024 May 10 00:24 .
-rwx------. 1 admin gadmin 398 May 10 00:25 authorized_keys
```

In this example, the Linux admin user is named `admin`

Step 5 Switch to the root user in a bash shell:

```
# sudo -i
```

Step 6 Update the sshd_config file:

a) Copy the current and original versions of the sshd_config file, located in the /etc/ssh directory:

```
# cp /etc/ssh/sshd_config /etc/ssh/sshd_config.orig
```

b) Open the sshd_config file in a vi editor:

```
# vi /etc/ssh/sshd_config
```

c) Enter the following key-value pairs:

```
Protocol 2
MaxAuthTries 3
PasswordAuthentication no
PermitRootLogin no
AuthenticationMethods publickey
PubkeyAuthentication yes
```

Important The default sshd_config file may already specify some of these key-value pairs. If this is the case, either:

- Change any values that do not match the ones listed above.
- Comment out the existing key-value pairs and specify the required entries on new lines.

Doing so will prevent conflicting or duplicate key-value pairs.

d) Save the file.

Step 7 Reload sshd:

```
# systemctl reload sshd.service
```

Caution Do not restart sshd. If any of the previous configuration steps are not completed correctly and you restart sshd, you will lose access to SSH. It is much safer to reload sshd because current SSH sessions are maintained (allowing you to make any necessary corrections).

The configuration of SSH authentication is complete. To confirm that configuration was successful, keep the existing SSH session open (in case you need to fix something) and try to open a new SSH session using the private key and passphrase you created in Step 3 of this procedure.

Harden NTP

Network Time Protocol (NTP) authenticates server date and time updates. We recommend you configure the Cisco EPN Manager server to perform time synchronization over NTP. Failure to manage NTP synchronization across your network can result in anomalous results. Management of network time accuracy is an extensive subject that involves your organization's network architecture and falls outside the scope of this guide. For more information on this topic, see (for example) the Cisco white paper Network Time Protocol: Best Practices.

Note the following:

- Because using NTP creates the possibility of security breach-related disruptions, you should also harden the NTP aspect of the Cisco EPN Manager server by using NTP version 4 (NTPv4). Cisco EPN Manager also supports NTPv3 because NTPv4 is backward compatible with NTPv3.
- You can configure a maximum of 5 NTP servers with Cisco EPN Manager .
- IPv6 support is not available for NTP.

Set Up NTP on the Cisco EPN Manager Server

To use the Network Time Protocol (NTP) to synchronize clocks on the server and network devices using an NTP server, NTP must first be set up on the Cisco EPN Manager server. For information on how to do this, see Set Up NTP on the Server, on page 765.

Enable Authenticated NTP Updates

Complete the following procedure to set up authenticated NTP updates:

Step 1 Log in to Cisco EPN Manager using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter config mode.

Step 3 Enter the following command to setup an external NTPv4 server:

```
ntp server serverIP ntp-key-id ntp-type password
```

Where:

- *serverIP* is the IP address of the authenticating NTPv4 server you want to use
- *ntp-key-id* is the md5 key id of the NTPv4 server
- *ntp-type* can be plain or hash
- *password* is the corresponding plain-text md5 password for the NTPv4 server

For example:

```
ntp server 209.165.202.128 20 plain myPass123
```

Or,

```
ntp server 209.165.202.128 20 hash myPass123
```

Step 4 Perform these tests to ensure NTP authentication is working correctly:

a) Check the NTP update details:

```
show run
```

b) Check NTP sync details:

```
show ntp
```

Configure External NFS-Based Storage Servers

NFS servers may be used as external storage in a Cisco EPN Manager installation, especially for data backup. Since NFS does not have built-in security, you must implement as many of the following security measures as possible to secure the NFS server:

- Set up a firewall in front of the NFS server—To do this practically, tie down the ports that NFS will use in various configuration files and then specify those ports in the firewall configurations.
- Use a port mapper—On the NFS server, only allow NFS transactions that involve specific IP addresses.
- To prevent attacks via a compromised DNS, only specify IP addresses (and not domain names) when configuring NFS.
- When setting up the export of folders, use the **root_squash** option in the /etc/exports file.
- When configuring the /etc/exports file, use the **secure** option.
- When configuring the backup staging and storage folders, use the **nosuid** and **noexec mount** options.

Note It is not mandatory to configure a staging folder.

- For the storage folder (and optional staging folder), configure a file access permission value of **755** (which grants all users read and write privileges) and set userid **65534** (the user **nobody**, who does not have any system privileges) as the owner.
- Tunnel NFS traffic either through SSH or SSL/TLS. For SSH, use RSA key-based authentication instead of user authentication.

Do not rely on just one of these measures to secure your NFS-based storage. Your best bet is to implement the combination of measures that best suits your situation. Also keep in mind that this list is not an exhaustive one. To achieve a higher level of confidence when hardening your storage, we recommend that you discuss your situation with a Linux system admin and a security expert beforehand.

Create Admin User

To create an admin user :

Step 1 Log in as the Linux CLI admin user and access the shell.

Step 2 Enter the following command to create a user:

This is an example:

```
admin(config)# username xyzabc password plain Text1234 role network-admin
```

Where,

- **xyzabc** can be the desired username
- **plain Text1234** can be the password in plain text
- **network-admin** can be the assigned role for the user

By default, the password being configured must contain at least 6 alpha numeric characters. It must have at least one character each in upper and lower case. The password cannot contain the username or the word cisco in it. You can modify the password policy to include special charters with the following limitations:

- You can use the special characters % (percent), , (comma), < (less-than), > (greater-than), and | (pipe) when password is enclosed within double quotes. For example: `"Test123%|"`.
- The special characters " (quotation), ? (question mark), \ (backslash), and ` (grave accent) are not supported in the password field.
- Other special characters, such as # (hash), * (asterisk), : (colon) and so on can be used without enclosing in double quotes.

CSDL Process

Cisco EPN Manager development adheres to the Cisco Secure Development Lifecycle (CSDL) process. This covers the entire development-to-deployment timespan to improve product and installation security. Cisco EPN Manager's product design is reviewed from a security viewpoint against specific criteria and the product is tested using security tools and test methods. In addition, Cisco EPN Manager is reviewed by external security experts and penetration testers. See Cisco Security Issue Resolution Process for a description of how security fixes are deployed (as part of the Cisco EPN Manager update lifecycle).

Cisco Security Issue Resolution Process

There are 2 types of defects and vulnerabilities: customer-found and Cisco-found. Let's cover how Cisco addresses them for Cisco EPN Manager.

Customer-Found Defects and Vulnerabilities

1. After a customer raises a service request with the Cisco Technical Assistance Center (TAC), the Cisco TAC opens a case with the support team who (depending on the problem) may open a Cisco Defect and Enhancement Tracking System (CDETS) defect report.
2. Cisco evaluates the defect to determine whether that defect poses a security risk to Cisco EPN Manager. If the defect does pose a security risk, then Cisco categorizes it as a vulnerability. Otherwise, Cisco treats the defect as a regular software defect.
3. Cisco does one of the following:
   - For security vulnerabilities, Cisco reports it to the Cisco Product Security Incident Response Team (PSIRT), develops a fix that adheres to Cisco PSIRT guidelines, and then allows Cisco PSIRT to handle both the disclosure of the vulnerability to the client and delivery of the patch.
   - For defects, Cisco determines its severity and schedules the release of a fix.

Cisco-Found Defects and Vulnerabilities

For the first year following the end-of-sale date for a Cisco EPN Manager version, Cisco provides bug fixes, maintenance releases, workarounds, or patches for critical bugs and security vulnerabilities reported via the TACS or Cisco.com Web site.

Two-Factor Authentication

The Two-Factor Authentication feature provides a two step authentication process to login to Cisco EPN Manager. Cisco EPN Manager supports two-factor authentication of a user through Cisco ACS server over RADIUS protocol. Cisco ACS supports the RSA SecurID server as external database.

The two-factor authentication consists of a two step validation of the user's PIN and an individually registered RSA SecurID token. When the user enters the correct token code along with a PIN, authentication is successful and the user is allowed to login to Cisco EPN Manager.

Prerequisites to enable Two-factor authentication in Cisco EPN Manager

- Cisco EPN Manager - version 3.0.1 and above
- Cisco ACS server with valid license - version 5.x
- RSA Server with valid license - version 8.4
- RSA Client tool - latest version

Enable Two-Factor Authentication in Cisco EPN Manager

To enable Two-factor authentication in Cisco EPN Manager, complete the following tasks:

- Configure RSA server for two-factor authentication, on page 727
- Sync RSA server with Cisco ACS Server , on page 728
- Add Cisco EPN Manager as Client in Cisco ACS Server, on page 729
- Add RADIUS Server Details in Cisco EPN Manager, on page 730

Configure RSA server for two-factor authentication

Cisco Secure ACS supports the RSA SecurID server as an external database.

RSA SecurID two-factor authentication consists of the user's personal identification number (PIN) and an individually registered RSA SecurID token that generates single-use token codes based on a time code algorithm.

A different token code is generated at fixed intervals, usually every 30 or 60 seconds. The RSA SecurID server validates this dynamic authentication code. Each RSA SecurID token is unique, and it is not possible to predict the value of a future token based on past tokens.

You can integrate a Cisco ACS 5.x server with RSA SecurID server authentication over RADIUS protocol.

To configure RSA server for two-factor authentication, complete the following tasks:

- Add Users to RSA Server , on page 728
- Assign Tokens to a User in RSA Server, on page 728

Add Users to RSA Server

To add users to the RSA server:

Step 1 In the Security Console, click **Identity** > **Users** > **Add New**.

Step 2 In the **Administrative Control** section, from the **Security Domain** drop-down list,select **System Domain**.

Step 3 In the **User Basics** section, do the following:

a) (Optional) In the **First Name** field, enter the user's first name. Do not exceed 255 characters.

b) (Optional) In the **Middle Name** field, enter the user's middle name. Do not exceed 255 characters.

c) In the **Last Name** field, enter the last name of the user. Do not exceed 255 characters.

d) In the **User ID** field, enter the User ID for the user. The User ID cannot exceed 48 characters.

Step 4 In the Password section, do the following:

a) In the **Password** field, enter a password for the user. This is the user's identity source password.

b) In the **Confirm Password** field, enter the same password that you entered in the **Password** field.

Step 5 In the **Account Information** section, do the following:

a) From the **Account Starts** drop-down lists, select the date and time you want the user's account to become active. The time zone is determined by local system time.

b) From the **Account Expires** drop-down lists, select the date and time you want the user's account to expire, or configure the account with no expiration date. The time zone is determined by local system time.

Step 6 Click **Save**.

Assign Tokens to a User in RSA Server

Assigning a token associates the token with a specific user. To assign tokens to a user:

Before you begin

Ensure an active user record exists in RSA server for each user to whom you want to assign a token.

Step 1 In the **Security Console**, click **Identity** > > **Users** > **Manage Existing**.

Step 2 Use the search fields to find the user(s) to whom you want to assign tokens.

Step 3 From the search results, click the user(s) to whom you want to assign tokens.

Step 4 From the context menu, under SecurID Tokens, click **Assign More**.

Step 5 From the list of available RSA SecurID tokens on the **Assign to Users** page, select the **Free SecureID Software Token** checkbox.

Step 6 Click **Assign**.

Sync RSA server with Cisco ACS Server

Complete the following tasks to sync RSA server with Cisco ACS Server.

- Generate Configuration File on RSA Server , on page 729

• Configure RSA Server on Cisco ACS Server, on page 729

Generate Configuration File on RSA Server

This procedure describes how the RSA SecurID server administrator creates authentication agents and a configuration file. An authentication agent is a Domain Name Server (DNS) name and an IP address of a device, software, or service that has rights to access the RSA database. The configuration file describes RSA topology and communication. Follow this procedure to generate the sdconf.rec file, which you will need to complete configuration tasks on Cisco ACS server.

Step 1 In the RSA Security Console, navigate to **Access** > > **Authentication Agents** > **Add New**.

Step 2 In the **Add New Authentication Agent** window, define a **Hostname** and **IP Address** for each agent you are adding.

Step 3 In the **Authentication Agent Attributes** window, define the **Agent Type** as **Standard Agent**.

Step 4 Navigate to **Access > Authentication Agents > Generate Configuration File** to generate the sdconf.rec file and click **Generate Configuration File**. Use the default values **Maximum Retries** and **Maximum Time Between Each Retry**.

Step 5 Click **Download Now** to download the configuration file. When prompted, click **Save to Disk** to save the ZIP file to your local machine. The .zip file contains the actual configuration sdconf.rec file.

Configure RSA Server on Cisco ACS Server

This procedure describes how to retrieve the sdconf.rec configuration file and submit it in Cisco ACS server.

Before you begin

Ensure you have generated the sdconf.rec file on the RSA server.

Step 1 In the Cisco Secure ACS Version 5.x console, navigate to **Users and Identity Stores** > **External Identity Stores** > **RSA SecurID Token Servers**, and click **Create**.

Step 2 Enter the name of the RSA server, and browse to the sdconf.rec file that was downloaded from the RSA server.

Step 3 Select the file, and click **Submit**.

Step 4 Map the RSA Server by navigating to **Access Policies** > **Identity** > **Select**, select the checkbox **Single result Selection**. In the **Identity Source** field, select the name of the RSA server and click **Select**.

Step 5 Configure RADIUS client devices to direct authentication requests. Navigate to **Users and Identity Stores** > **External Identity Stores** > **RADIUS Identity Servers**.

Step 6 Under the **General** tab, enter the name of the RSA RADIUS Identity Server. Under the **Primary Server** area, enter details of the server in the **Hostname AAA**, **Shared Secret**, **Authentication port**, **Server Timeout**, **Connection Attempts fields**.

Add Cisco EPN Manager as Client in Cisco ACS Server

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Network Resources** > > **Network Devices** > **Network Devices and AAA Clients**.

Step 3 In the **Network Devices** page, click **Create**.

Step 4 Enter the device name and IP address of the Cisco EPN Manager server.

Step 5 Choose the authentication option as RADIUS, and enter the shared secret.

Ensure that this shared secret matches the shared secret you enter when adding the Cisco ACS server as the RADIUS server in Cisco EPN Manager.

Step 6 Click **Submit**.

Add RADIUS Server Details in Cisco EPN Manager

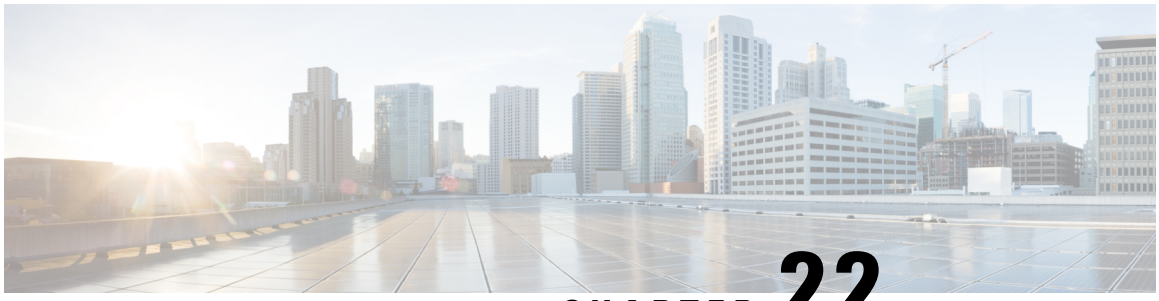
Use the following procedures to add the Cisco ACS Server details and configure RADIUS mode on Cisco EPN Manager.

- Add a RADIUS or TACACS+ Server to Cisco EPN Manager, on page 824
- Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server, on page 825

Two-factor Authentication Workflow

The steps in Cisco EPN Manager two-factor authentication workflow are listed below:

1. In the first login to Cisco EPN Manager, based on the mode defined in RSA Server (user-defined-pin or pin-generated-by-system), a unique PIN is generated that the user will have to remember. User enters this PIN in RSA SecurID client tool to generate RSA SecureID token.
2. In the Cisco EPN Manager login page, user enters username and RSA SecureID token (generated from Step 1).
3. Cisco EPN Manager sends the login request with username and token details to Cisco ACS server over RADIUS protocol .
4. Cisco ACS Server forwards the login request to RSA server.
5. RSA server authenticates the user details and confirms successful user authentication to Cisco ACS server.
6. Cisco ACS server matches the user to the authorization profile configured and allows the user to login to Cisco EPN Manager.



CHAPTER 22

Backup and Restore

Backup and Restore Concepts

Backup Types: Application and Appliance

Cisco EPN Manager supports two types of backups:

- Application backups—Contain Cisco EPN Manager application data but do not include platform data (host-specific settings, such as the server hostname and IP address). Application backup should be used during Cisco EPN Manager upgrade, when you want to move only application data and not the platform/host specific configurations.
- Appliance backups—Contain all application data and platform data (host-specific settings, including the hostname, IP address, subnet mask, default gateway, and so on). Appliance backup should be used for disaster recovery (or to recover from platform hardware or software failures). For example, to recover from any disk or filesystem failure, the standard recovery process would be to re-install Cisco EPN Manager and then restore from the appliance backup in order to restore all data as well as platform-specific configurations. You would then need to manually reconstruct the HA configurations as they are not included in the appliance backup.

Note For details on what is considered application data and what is considered platform data, see Information That Is Backed Up, on page 734.

Note the following about application and appliance backups.

- Application and appliance backups can be restored to the same or a new host, as long as the new host has the same hardware and software configuration as the host from which the backup was taken.
- You can only restore an appliance backup to a host running the same version of the Cisco EPN Manager server software as the server from which the backup was taken.
- When upgrading to a later version of Cisco EPN Manager, application backup and restore can run across different releases, as long as the upgrade path is supported.
- You cannot restore an application backup using the appliance restore command, nor can you restore an appliance backup using the application restore command.

We recommend the following best practices:

- If you are *evaluating* Cisco EPN Manager, use the default automatic application backup to the local repository.
- If you are running Cisco EPN Manager *in a production environment* as a virtual appliance, take regular application backups to a remote backup server. You can use the application backups to restore your server for all failures except complete failure of the server hardware.

Backup Scheduling

Cisco EPN Manager performs automatic scheduled application backups. This feature is enabled by default and creates one application backup file every day in the default local backup repository.

You can change this schedule as needed. You can also take an automatic application backup at any time from the web GUI. Appliance backups can only be taken from the command line.

Automatic application backups can create storage space problems if the backup repository is local to the Cisco EPN Manager server. While this is usually acceptable in test implementations, it is not intended to substitute for routine scheduled backups to remote servers in a production environment.

We recommend the following for production environments:

- Set up remote repositories to store the backup files.
- Use the automatic schedule application backup to create backups on the remote repositories on a regular schedule.

Even if you are using scheduled backups, you can still use the command line to create application or appliance backups at any time.

Note By default, two minutes are added to the job execution time for job creation.

Backup Repositories

By default, automatic application backup feature stores backup files in the local backup repository **/localdisk/defaultRepo**. You can use the web GUI to create a new local backup repository and then choose it when you set up automatic application backups. You can also specify a remote repository but you must create the repository first as described in Set Up and Manage Repositories, on page 736.

When taking application or appliance backups using the command line, you must specify the local or remote repository you want the backup to be stored in. In a production environment, this is normally a remote repository that is accessed via NFS, SFTP, or FTP. We recommend you use NFS because it is typically much faster and more reliable than other protocols.

There is no difference between performing an application backup from the command line or performing it from the web GUI. Both actions create the same backup file.

Whenever you use NFS to take backups or restore data from a remote backup, make sure the mounted NFS server remains active throughout the backup or restore operation. If the NFS server shuts down at any point in the process, the backup or restore operation will hang without warning or an error message.

Backup Filenames

Application backups launched from the web GUI—either automatically or manually—are assigned a filename with the following format:

*host-yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_APP_CK*checksum*.tar.gpg

Application backups launched from the CLI use the same format, except that the file starts with the user-specified filename rather than the server name.

filename*-yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_APP_CK*checksum*.tar.gpg

Appliance backups launched from the CLI have files that also start with the user-specified filename, but the type is indicated as SYS, not APP.

filename*-yymmdd-hhmm*_VER*ver*_BKSZ*size*_CPU*cpus*_MEM*target*_RAM*ram*_SWAP*swap*_**SYS**_CK*checksum*.tar.gpg

The following table describes the variables used by the backup files.

Variable	Description
host	Host name of the server from which the backup was taken (for application backups launched from web GUI).
filename	Filename specified by user in command line (for application backups launched from CLI, and for appliance backups)
yymmdd-hhmm	Date and time the backup was taken
ver	Internal version.
size	Total size of the backup
cpus	Total number of CPUs in the server from which the backup was taken
target	Total amount of system memory in the server from which the backup was taken
ram	Total amount of RAM in the server from which the backup was taken

swap	Total size of the swap disk on the server from which the backup was taken
checksum	Backup file checksum

Backup Validation Process

Cisco EPN Manager performs the following steps to validate the backup files:

1. Before starting the backup process, validates disk size, fast-recovery area, and control files.
2. Validates the created backup database to ensure that it can be restored.
3. Validates the zipped application data against the files that were backed up.
4. Validates the TAR file to make sure it is correct and complete.
5. Validates the GPG file to ensure that it is correct.

If you manually transfer the backup file, or if you want to verify that the backup file transfer is completed, view the file's md5CheckSum and file size.

Another best practice for validating a backup is to restore it to a standalone "test" installation of Cisco EPN Manager.

Information That Is Backed Up

The following table describes the information that is contained in backup files. This information is restored to the server from backups.

See Information That Is Not Backed Up, on page 736 for details about data that is not saved by the backup mechanism.

Note The /opt/CSCOlumos/conf/Migration.xml file contains all configuration files and reports that are backed up. This file is included in the backup and is restored.

Data Type	Feature	Information Saved and Restored

Application Data	Background job settings	Data in the database
	Configuration archive (device configuration files)	Data in the database
	Configuration templates	• Files in /opt/CSCOlumos: • /conf/ootb • /xmp_inventory/dar/customized-feature-parts/CONFIGURATION • Data in the database
	Credentials	Data in the database
	Device inventory data	Data in the database
	Licenses	Files in /opt/CSCOlumos/licenses
	Maps	• Files in /opt/CSCOlumos/domainmaps • Data in the database
	Reports	• Files in /localdisk/ftp: • /reports • /reportsOnDemand • Data in the database
	Managed device software image files	Data in the database
	System settings	Data in the database
	User preferences	• Files in /opt/CSCOlumos/conf/wap/datastore/webacs/xml/prefs • Data in the database
	CEPNM users, groups, and roles	Data in the database
	Virtual domains	Data in the database

Platform Data	CLI settings	All CLI information and settings are preserved. This includes the list of backup repositories, the FTP user name, users created using the CLI, AAA information specified via the CLI, and other CLI settings (such as the terminal timeout).
	Credentials	Linux OS credentials file
	Network settings	Files in /opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml
	Linux user preferences	Linux data structure
	Linux users, groups, and roles	Linux data structure

Information That Is Not Backed Up

Before performing a backup, make sure that you manually note the following information because it is not saved as part of the backup process. You will need to reconfigure these settings after the data has been restored.

- High availability configurations
- Local customization (for example, report heap size)
- Patch history information
- Certificates

  If you have configured a server with a web certificate and set it up to authenticate clients with client certificates, you need to repeat the same configuration on the new server again after you have completed the backup and restore procedure.

For a list of information that is backed up, see Information That Is Backed Up, on page 734.

Set Up and Manage Repositories

Cisco EPN Manager supports the following repository types:

- Remote repositories—NFS, FTP, SFTP, and TFTP.

See the following topics for information on how to set up and manage these different types of repositories.

Create a Local Backup Repository

Cisco EPN Manager stores automatic backup files in the default local backup repository **/localdisk/defaultRepo**. You can create a different local backup repository and use it if you prefer.

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 Choose **System Jobs** > **Infrastructure**.

Step 3 In the Jobs list, check the **Server Backup** check box.

Step 4 Click **Edit** (the pencil icon) to open the Edit Job Properties dialog box.

Step 5 Create the new local repository using the Edit Job properties dialog box.

a. Click **Create**. The Create Backup Repository dialog box opens.

b. Enter the name of the local repository you want to create.

c. Enter the password if you want to make the backup password secured.

Note Make sure you remember the password to restore the backup.

d. If it is an FTP repository, check the **FTP** check box and enter the location and credentials.

e. Click **Submit**. The new repository is added to the Backup Repository drop-down list in the Edit Job Properties dialog box.

Step 6 Click **Save**.

Step 7 If you want to use the repository for future automatic application backups, specify it as described in Specify the Backup Repository for Automatic Backups, on page 743.

Use a Remote Backup Repository

In production environments, we recommend that you use remote repositories for backups so that your network management data is protected from hardware and site failures. In most cases, this means you will need to:

1. Create one or more remote repositories to hold Cisco EPN Manager backup files. You will need to set these up yourself if your organization does not already have remote backup servers.
2. Specify the remote repository as the destination for automatic application backups.
3. If needed, specify the interval between automatic application backups and time of day to take them. You will need to monitor and manually archive automatic application backups stored on remote repositories (because the **Max backups to keep** setting does not apply to remote repositories).
4. Specify the remote repository as the backup destination when taking an application or appliance backup using the CLI backup commands.

As with any resource that you plan to access remotely, specifying the correct server IP address and login credentials during setup are a requirement for successful use of remote backup repositories with Cisco EPN Manager.

Use Remote NFS Backup Repositories

To use NFS-based remote backup repositories, you need an NFS file server (which exports the designated folders in its file system to its client) and Cisco EPN Manager (which acts as the server's client). The Cisco EPN Manager system mounts the exported folders and makes them, along with other local folders, available to the Cisco EPN Manager server. To set this up, complete the following three tasks:

1. Specify the paths for the two folders on the NFS server that will stage and store backups, then configure the NFS server to export these paths. Since this falls outside of the scope of Cisco EPN Manager setup, this task should be completed by the NFS server’s system admin.

2. Set up Cisco EPN Manager to use the staging and storing folders you specified. This should be completed by a Cisco EPN Manager admin.
3. Secure communication between the NFS server and Cisco EPN Manager, which is very important because NFS is not secure on its own. This should be completed by a Linux admin who has a solid understanding of the security issues that NFS and its installation entails. For tips on hardening NFS, see Harden NFS-Based Storage.

Before You Set Up the NFS Backup Configuration

Before you begin, make sure:

- You know the IP address of the NFS server on which you want to stage and store backups. The staging and storage folders can be on the same NFS server, or on separate NFS servers. If you plan to stage and store on separate NFS servers, you will need IP addresses for both servers.
- You know the path names of the staging and storage folders on the NFS server. If you choose to stage and store on the same NFS server, the staging and storage folders *must* have different names.
- You have an administrator user ID with root privileges on the Cisco EPN Manager server.
- You have selected a repository name on the Cisco EPN Manager server, which will point to the NFS server storage folder.

Set Up NFS-Based Remote Repositories

Complete the following procedure to set up the NFS-based remote repositories that Cisco EPN Manager use for backups.

Step 1 Log in to the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter configuration mode:

```
configure terminal
config#
```

Step 3 Set up the NFS remote repositories that stage the temporary files that are created during backup processing and store completed backup files:

```
config# backup-staging-url nfs://Staging_Server_IP_Address:/Staging_Server_Path
config# repository repositoryName
config-Repository# url nfs://Storage_Server_IP_Address:/Storage_Server_Path
```

Where:

- *Staging_cdg_Server_IP_Address* is the IP address of the NFS server on which the staging repository is located.
- *Staging_Server_Path* is the full path of the staging repository on its host NFS server.
- *repositoryName* is the name of the remote repository that will store completed backup files.
- *Storage_cdg_Server_IP_Address* is the IP address of the NFS server on which the storage repository is located.
- *Storage_Server_Path* is the full path of the storage repository on its host NFS server.

Caution We recommend that you only enter an IP address for *Staging_cdg_Server_IP_Address* and *Storage_cdg_Server_IP_Address*. If the DNS service has been compromised and you enter a URL instead, this can result in the redirection of traffic to a malicious NFS server. That said, if you still prefer to specify a URL, we suggest you configure Cisco EPN Manager to use local name resolution (instead of relying on the DNS service). This can be done by entering the NFS server's name and IP address in the **/etc/hosts** file. Doing so can improve system security.

Step 4 Exit configuration mode:

```
config-Repository# exit
config# exit
```

Use Remote FTP Backup Repositories

Note We recommend using remote NFS repositories.

You can create backup repositories on a remote FTP server and configure the Cisco EPN Manager server to use them.

The FTP server hosting your backups can be set up anywhere in your network, as long as the server:

- Has an IP address accessible from the Cisco EPN Manager server.
- Has a user (FTP user) with write access to the FTP server disk.
- Has a local subdirectory that matches the repository name you specify on the Cisco EPN Manager server.
- Has a password of 16 characters or less.

Other than these requirements, no other configuration is needed on the FTP backup server.

For the SFTP server details to appear in the **Backup Repository** drop-down list in the web GUI, you should configure the FTP server using the CLI. You can configure the FTP server only using the CLI.

Step 1 Log into the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter configuration mode:

```
configure terminal
config#
```

Step 3 Configure a symbolic link to the remote FTP server, then exit configuration mode:

```
config# repository repositoryName
config-Repository# url ftp://RemoteServerIP//sharedFolder
config-Repository# user userName password plain userPassword
config-Repository# exit
config# exit
```

Where:

- *repositoryName* is the name of the repository (for example, **MyRepo** or **EPNManager**).

- *RemoteServerIP* is the IP address of the FTP server hosting the shared backup folder.
- *sharedFolder* is the name of the shared backup folder on the FTP server.
- *userName* is the name of the user with write privileges to the repository on the FTP server.
- *userPassword* is the corresponding password for that user. The password must be 16 characters or less.

Step 4 Verify the creation of the symbolic link:

```
show repository repositoryName
```

What to do next

When you perform a manual backup, specify the new repository as the repository name in the backup command. For example:

```
backup MyBackupFileName repository MyRepo application NCS
```

If you want to use this repository for automatic backups, see Specify the Backup Repository for Automatic Backups, on page 743.

Use Remote SFTP Backup Repositories

Note We recommend using remote NFS repositories.

You can create backup repositories on a remote SFTP server and configure the Cisco EPN Manager server to use them.

The SFTP server hosting your backups can be set up anywhere in your network, as long as the server:

- Has an IP address accessible from the Cisco EPN Manager server.
- Has a user with write access to the SFTP server disk.
- Has a local shared folder where the backups will be stored.

Other than these requirements, no other configuration is needed on the SFTP backup server.

For the SFTP server details to appear in the **Backup Repository** drop-down list in the web GUI, you should configure the SFTP server using the CLI. You can configure the SFTP server only using the CLI.

Step 1 Log into the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter configuration mode:

```
configure terminal
config#
```

Step 3 Configure a symbolic link to the remote SFTP server, then exit configuration mode:

```
config# repository repositoryName
config-Repository# url sftp://RemoteServerIP//sharedFolder
```

```
config-Repository# user userName password plain userPassword
config-Repository# exit
config# exit
```

Where:

- *repositoryName* is the name of the repository (for example, **MyRepo** or **EPNManager**).
- *RemoteServerIP* is the IP address of the SFTP server hosting the shared backup folder. Note that the example above specifies an absolute path to the shared folder. To specify a relative path to the shared folder, use only one slash in the URL (for example, **url sftp://***RemoteServerIP***/***sharedfolder*).
- *sharedFolder* is the name of the shared backup folder on the SFTP server.
- *userName* is the name of the user with write privileges to the repository on the SFTP server.
- *userPassword* is the corresponding password for that user.

Step 4 Verify the creation of the symbolic link:

```
show repository repositoryName
```

What to do next

When you perform a manual backup, specify the new repository as the repository name in the backup command. For example:

```
backup MyBackupFileName repository MyRepo application NCS
```

If you want to use this repository for automatic backups, see Specify the Backup Repository for Automatic Backups, on page 743.

Use Remote TFTP Backup Repositories

Note We recommend using remote TFTP repositories.

You can create backup repositories on a remote TFTP server and configure the Cisco EPN Manager server to use them.

The TFTP server hosting your backups can be set up anywhere in your network, as long as the server:

- Has an IP address accessible from the Cisco EPN Manager server.
- Has a user with the *write* access to the TFTP server disk.
- Has a local shared folder where the backups are stored.
- Has a remote TFTP server that is up and running.

Other than these requirements, no other configuration is needed on the TFTP backup server.

For the TFTP server details to appear in the **Backup Repository** drop-down list in the web GUI, you should configure the TFTP server using the CLI. You can configure the TFTP server only using the CLI.

Step 1 Log in to the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter the configuration mode.

Step 3 Configure a symbolic link to the remote TFTP server, then exit the configuration mode:

```
config# repository repositoryName
config-Repository# url tftp://RemoteTFTPServerIP/sharedFolder
config-Repository# exit
config# write memory
config# exit
```

Where,

- *repositoryName* is the name of the repository (for example, **MyRepo** or **EPNManager**).
- *RemoteTFTPServerIP* is the IP address of the TFTP server hosting the shared backup folder.

  Note The example above specifies an absolute path to the shared folder. To specify a relative path to the shared folder, use only one slash in URL (for example, url tftp://RemoteServerIP/sharedfolder).

- *sharedFolder* is the name of the shared backup folder on the TFTP server.
- *write memory* is the command that is used to save configuration.

Step 4 Verify the creation of the symbolic link:

```
show repository repositoryName
```

What to do next

When you perform a manual backup, specify the new repository as the repository name in the backup command. For example:

```
backup MyBackupFileName repository MyRepo application NCS
```

If you want to use this repository for automatic backups, see Specify the Backup Repository for Automatic Backups, on page 743.

Delete a Local Backup Repository

Use the following procedure to delete a local backup repository. This procedure ensures that the admin interface has the updated information.

Step 1 Log into the server as a Cisco EPN Manager CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Step 2 List the local application backup repositories and identify the one that you want to delete:

```
show running-config | begin repository
```

Step 3 Enter configuration mode and delete the repository:

```
configure terminal
(config)# no repository repositoryName
```

Step 4 Repeat step 2 to verify that the repository was deleted.

Set Up Automatic Application Backups

Automatic application backups are enabled by default after installation. You can customize the schedule, specify a different backup repository, or adjust the number of backups that are saved.

To check what data is saved by the backup mechanism (and verify whether you need to manually save any data that is not backed up), see these topics:

- Information That Is Backed Up, on page 734
- Information That Is Not Backed Up, on page 736

Schedule Automatic Application Backups

Automatic application backups are enabled by default but you can adjust the day and interval at which these backups are performed. Performing a backup is resource-intensive and affects Cisco EPN Manager server performance. Avoid scheduling automatic backups to occur at peak traffic times.

If an automatic application backup fails, Cisco EPN Manager generates a Backup Failure alarm (with major severity). You can view these alarms just as you do other alarms (see Find and View Alarms, on page 252).

Note After an automatic application backup fails, a pop-up message is displayed before every subsequent login attempt. This message will continue to appear until you acknowledge the corresponding alarm.

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 Choose **System Jobs** > **Infrastructure**.

Step 3 In the Jobs list, check the **Server Backup** check box, then click **Edit Schedule**. The Schedule dialog box opens.

Step 4 In the Schedule dialog box, select a start date, recurrence interval, and optional end time.

Step 5 Click **Submit**. These settings will now be used for future automatic application backups.

Specify the Backup Repository for Automatic Backups

You can use the Cisco EPN Manager interface to specify a different backup repository for automatic application backups. The backup repository can be local or remote. You can also use the interface to create a new local backup repository if it does not already exist.

Before you begin

If you want to use a remote repository for automatic backups, you must create the repository first. Only local repositories can be created using this procedure. See Set Up and Manage Repositories, on page 736.

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 Choose **System Jobs** > **Infrastructure**.

Step 3 In the list of jobs, check the **Server Backup** check box.

Step 4 Click **Edit** (the pencil icon). The Edit Job Properties dialog box opens.

Step 5 Select a repository from the Backup Repository drop-down list, then click **Save**. Cisco EPN Manager will use the new repository when it performs the next automatic application backup.

Change the Number of Automatic Application Backups That Are Saved

Follow this procedure to adjust the number of automatic application backups that are saved on a local repository. When a backup exceeds the number you specify here, Cisco EPN Manager deletes the oldest backup from the repository.

The **Max UI backups to keep** setting does not apply if you are using remote repositories for automatic application backups. You must monitor and archive or delete old backups on remote repositories using your own methods.

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 Choose **System Jobs** > **Infrastructure**.

Step 3 In the Jobs list, check the **Server Backup** check box.

Step 4 Click **Edit** (the pencil icon) to open the Edit Job Properties dialog box.

Step 5 Enter a value in the **Max UI backups to keep** field, then click **Save**. Cisco EPN Manager will enforce this setting at the next backup.

Perform a Manual Backup

The topics in this section explain how to perform manual application or appliance backups.

To check what data is saved by the backup mechanism (and verify whether you need to manually save any data that is not backed up), see these topics:

- Information That Is Backed Up, on page 734
- Information That Is Not Backed Up, on page 736

Perform an Immediate Application Backup

Cisco EPN Manager performs automatic application backups as described in Backup Scheduling, on page 732. If needed, you can manually trigger an application backup as described in the following topics.

Perform an Immediate Application Backup Using the Web GUI

Use this procedure to trigger an immediate application backup using the web GUI.

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard**.

Step 2 Choose **System Jobs** > **Infrastructure**.

Step 3 In the Jobs list, check the **Server Backup** check box, then click **Run**.

Step 4 To view the backup status, scroll to the top of the table to locate the new job, then check its status and results.

Perform an Immediate Application Backup Using the CLI

Use this procedure to trigger an immediate application backup using the CLI.

Step 1 Log into the server as a Cisco EPN Manager CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Step 2 Display the list of backups, where *repositoryName* is the backup repository:

```
show repository repositoryName
```

Step 3 Start the remote backup.

```
backup filename repository repositoryName application NCS
```

where, *filename* is the name that you want to give the application backup file (for example, myBackup). The character length of the file name is 26. Other information is appended to the filename automatically, as explained in Backup Filenames, on page 733.

Perform a Manual Appliance Backup

Use this procedure to perform an appliance backup to a remote repository. Be sure you have configured the remote repository as described in Set Up NFS-Based Remote Repositories, on page 738.

Step 1 Make sure the remote host is available.

Step 2 Log into the Cisco EPN Manager server as admin (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Step 3 Start the remote backup:

```
(admin)# backup filename repository repositoryName
```

Step 4 To verify that the backup transfer is complete, view the md5CheckSum and file size.

Restore Cisco EPN Manager Data

All restore operations are performed using the CLI. Data can be restored to the host where the backup is executed (local host), or to a remote host. Backups can only be restored in their entirety; you cannot restore only parts of a backup.

For more information, see the following topics.

- Restore an Application Backup, on page 746
- Restore an Appliance Backup, on page 747

Restore an Application Backup

Note To restore an *appliance* backup, use the procedure in Restore an Appliance Backup, on page 747.

When you restore an application backup, make sure it is being restored to an OVA installation of the same size or larger. If the OVA installation is smaller, the restore will fail.

Before you begin

If you are using high availability, read the guidelines in Remove HA During Restore, on page 913 before restoring your data.

Step 1 Log in to the server as a Cisco EPN Manager CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Step 2 If a previous restoration attempt failed, the database may have been corrupted. Run this command to recreate the database:

```
ncs run reset db
```

Note High Availability (if enabled) must be removed before running this command.

Running the **ncs run reset db** command deletes the existing data in database (network data) and resets the database to default factory settings.

Step 3 List the saved application backups and identify the one that you want to restore. *repositoryName* is the repository that contains the backup files.

```
show repository repositoryName
```

Step 4 To restore the previously backed-up application data:

```
restore backupFileName repository repositoryName application NCS
```

Step 5 If you are using Cisco Smart Licensing, reregister Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. See Register Cisco EPN Manager with the Cisco Smart Software Manager, on page 701.

Restore an Appliance Backup

Note To restore an *application* backup, use the procedure in Restore an Application Backup, on page 746.

When you restore an appliance backup, make sure it is being restored to an OVA installation of the same size or larger. If the OVA installation is smaller, the restore fails.

Cisco recommends that you change the restored server's IP address, subnet mask, and default gateway if:

- The restored host is on the same subnet as the old host, and the old host is still active.
- The restored host is on a different subnet from the old host.

Before you begin

If you are using high availability, read the information in Remove HA During Restore, on page 913 before restoring your data.

Step 1 Log in to the server as a Cisco EPN Manager CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Step 2 If a previous restoration attempt failed, the database may have been corrupted. With the backup stored in an external repository, reinstall the setup using the same release and then retry the restore.

Step 3 List the saved appliance backups and identify the one that you want to restore. *repositoryName* is the repository that contains the backup files.

```
show repository repositoryName
```

Step 4 To restore the previously backed-up application data:

```
restore backupFileName repository repositoryName
```

Step 5 Determine whether you should change the IP address, subnet mask, and default gateway.

a) Check if your installation meets the following criteria:

- The restored host is on the same subnet as the old host, and the old host is still active.
- The restored host is on a different subnet from the old host.

If it does, perform the next step.

b) Change the IP address, subnet mask, default gateway and (optionally) the host name on the restored server.

c) Write the changes to the server's running configuration and restart Cisco EPN Manager services. For example:

```
configure terminal
(config)# int GigabitEthernet 0
(config-GigabitEthernet)# ip address IPAddress subnetMask
(config-GigabitEthernet)# exit
```

```
(config)# ip default-gateway gatewayIP
(config)# hostname hostname
(config)# exit
(admin)# write mem
(admin)# ncs stop
(admin)# ncs start
(admin)# exit
```

Step 6 If you are using Cisco Smart Licensing, reregister Cisco EPN Manager with the Cisco Smart Software Manager (CSSM) on Cisco.com. See Register Cisco EPN Manager with the Cisco Smart Software Manager, on page 701.

Recover from Failed Restores

You may sometimes find that a restore does not complete, or reports a failure. Whenever a restore fails, you run the risk of database corruption, which can prevent the further restoration or re-installation. Perform the following steps to restore a corrupted database before attempting another restore or re-installation.

Step 1 Open a CLI session with the Cisco EPN Manager server (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Step 2 Enter the following command to reset the corrupted database:

```
ncs run reset db
```

Manage Disk Space Issues During Backup and Restore

If you are experiencing disk issues *during* a backup or restore, move your installation to a server with adequate disk space by following the procedure in Migrate to Another Virtual Appliance Using Backup and Restore, on page 748.

If you are unable to create a backup *after* a restore of your existing system, follow the steps explained in Compact the Database, on page 773 to free disk space and create a successful backup. If you are still unable to create a backup after using the **ncs cleanup** command, set up and use a remote repository (using NFS, FTP, or SFTP) for your backups, as explained in Use a Remote Backup Repository, on page 737.

Migrate to Another Virtual Appliance Using Backup and Restore

You will need to migrate your Cisco EPN Manager data from an existing virtual appliance (OVA server installation) to a new one whenever you want to:

- Replace the old server entirely, such as after a catastrophic hardware failure. In this case, you can use your old installation media to re-create the new host on a replacement server, then migrate your application data from the old host to the new host.
- Migrate to a larger or more powerful server, so you can use Cisco EPN Manager to manage more of your network. In this case, you will want to ensure that you have the OVA installation file and install it on

the new server using the larger installation option before retiring the older, smaller one. You can then migrate your application data from the old host.

In both cases, it is relatively easy to migrate your old data to the new virtual appliance by restoring to the new host an appliance or application backup taken from the old host.

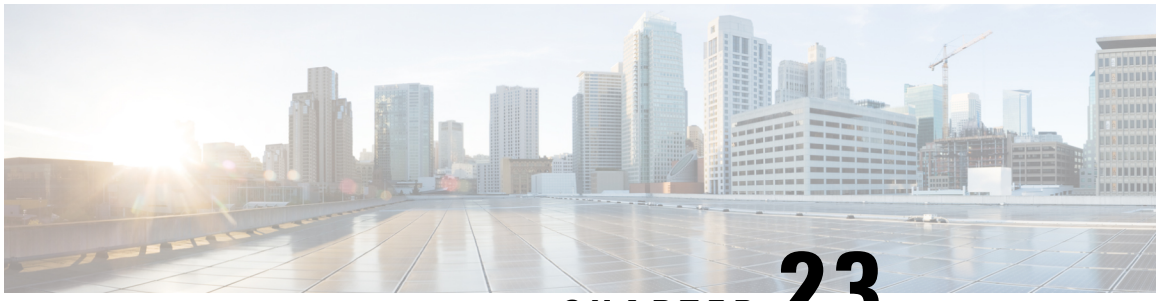
Step 1 If you have not already done so, set up a remote backup repository for the old host, as explained in Use a Remote Backup Repository, on page 737.

Step 2 Perform an application backup of the old host and save it to the remote repository (see Perform an Immediate Application Backup Using the CLI, on page 745).

Step 3 Install the new host (installation steps are in the Cisco Evolved Programmable Network Manager Installation Guide).

Step 4 Configure the new host to use the same remote backup repository as the old host (see Use a Remote Backup Repository, on page 737).

Step 5 Restore the application backup on the remote repository to the new host (see Restore an Application Backup, on page 746).



CHAPTER 23

Server Health and Configuration

View the Cisco EPN Manager Server Configuration

Use this procedure to view Cisco EPN Manager server configuration information such as the current server time, kernel version, operating system, hardware information, and so forth.

Step 1 Choose **Administration** > **Dashboards** > **System Monitoring Dashboard**.

Step 2 Click the **Overview** tab.

Step 3 Click **System Information** at the top left of the dashboard to expand the System Information field.

Change the Cisco EPN Manager Hostname

Cisco EPN Manager prompts you to enter a host name when you install the server. For a variety of reasons, you may find a mismatch between the host name configured on the Cisco EPN Manager server and the host name configured elsewhere. You can resolve this issue without re-installing Cisco EPN Manager by changing its host name on the server. To do so:

Note In some conditions, the files `tnsnames.ora` and `listener.ora` do not reflect the new hostname correctly after you change the host name. To avoid this, before you begin:

1. Make a back up of the following files on primary and secondary servers.
   - ./base/product/12.1.0/dbhome_1/network/admin/tnsnames.ora
   - ./base/product/12.1.0/dbhome_1/network/admin/listener.ora
   - /opt/oracle/templates/netcaxmp_prod.rsp
2. After the hostname change, use the three backup files to edit all occurrences of the host name to reflect the newly specified host name.
3. Restart the oracle listener (unless restart of Cisco EPN Manager is required and Step 2 can be performed when Cisco EPN Manager is down).

Step 1 Open a CLI session with the Cisco EPN Manager server, making sure you enter **configure terminal** mode.

See Connect via CLI.

Step 2 Enter the following command:

`Cisco_EPN_Manager_Server/admin(config)#` **hostname** *newHostName*

where *newHostName* is the host name you want to assign to the Cisco EPN Manager server.

Step 3 Restart the Cisco EPN Manager server using the **ncs stop** and **ncs start** commands.

Step 4 Check the host name configured for your SSL server certificate:

- If the host name is the same as the one you specified in Step 2, you can stop here.
- If the host name is different, you will need to create a new SSL server certificate configured with the host name you specified in Step 2 and then install it. .

Connect via CLI

Administrators can connect to the Cisco EPN Manager server via its command-line interface (CLI). CLI access is required when you need to run commands and processes accessible only via the Cisco EPN Manager CLI. These include commands to start the server, stop it, check on its status, and so on.

Before you begin

Before you begin, make sure you:

- Know the user ID and password of an administrative user with CLI access to that server or appliance. Unless specifically barred from doing so, all administrative users have CLI access.
- Know the IP address or host name of the Cisco EPN Manager server.

Step 1 Start up your SSH client, start an SSH session via your local machine's command line, or connect to the dedicated console on the Cisco EPN Manager physical or virtual appliance.

Step 2 Log in as appropriate: If you are using a GUI client: Enter the ID of an active administrator with CLI access and the IP address or host name of the Cisco EPN Manager server. Then initiate the connection. If you are using a command-line client or session: Log in with a command like the following:[localhost]# ssh username@IPHost -Whereusername is the user ID of a Cisco EPN Manager administrator with CLI access to the server. IPHost is the IP address or host name of the Cisco EPN Manager server or appliance. If you are using the console: A prompt is shown for the administrator user name. Enter the user name.

Cisco EPN Manager will then prompt you for the password for the administrator ID you entered.

Step 3 Enter the administrative ID password. Cisco EPN Manager will present a command prompt like the following:

```
Cisco_EPN_Manager_Server/admin#
```

Step 4 If the command you need to enter requires that you enter **configure terminal** mode, enter the following command at the prompt:

`Cisco_EPN_Manager_Server/admin#`**configure terminal**

The prompt will change from `Cisco_EPN_Manager_Server/admin#` to `Cisco_EPN_Manager_Server/admin/conf#`.

Secure the Connectivity of the Cisco EPN Manager Server

For data security, Cisco EPN Manager encrypts data in transit using standard public key cryptography methods and public key infrastructure (PKI). You can obtain more information about these technologies from the internet. Cisco EPN Manager encrypts the data that is exchanged between the following connections:

- Between the web server and the web client
- Between a CLI client and the Cisco EPN Manager CLI shell interface (handled by SSH)
- Between the Cisco EPN Manager and systems such as AAA and external storage

To secure communication between the web server and web client, use the public key cryptography services that are built in as part of the HTTPS mechanism. For that you need to generate a public key for the Cisco EPN Manager web server, store it on the server, and then share it with the web client. This can be done using the standard PKI certificate mechanism which not only shares the web server public key with the web client, but also guarantees that the public key belongs to the web server (URL) you are accessing. This prevents any third party from posing as the web server and collecting sensitive information that the web client is sending to the web server.

These topics provide additional steps you can take to secure the web server:

- Cisco recommends that the Cisco EPN Manager web server authenticate web clients using certificate-based authentication.
- To secure connectivity between a CLI client and the Cisco EPN Manager CLI interface, refer to the security hardening procedures in Harden the Cisco EPN Manager Web Server, on page 918.
- To secure connectivity between the Cisco EPN Manager and systems such as AAA and external storage, refer to the recommendations in Harden Your Cisco EPN Manager Storage, on page 923.

Set Up HTTPS to Secure the Connectivity of the Web Server

HTTPS operations use a server key that is generated using public key cryptography algorithms, and trust chain certificates that are generated using the server key. These certificates are applied to the Cisco EPN Manager web server. Depending upon how you generated the certificates, you may have to request the client browsers to trust these certificates the first time the browser connect s to the web server. The HTTPS mechanism ensures the security of the server machine (which in turn improves security of all other associated systems).

Signing Entity	Description	See:
Certificate Authority (CA) signed certificates	A Certificate Authority (CA) generates and issues these certificates. The certificates bind a public key to the name of the entity (for example, a server or device) that is identified in the certificate. You must generate a Certificate Signing Request (CSR) file from the Cisco EPN Manager server, and submit the CSR file (which contains the server key) to the CA. When you receive the certificates, you apply them to the web server. These certificates can be generated by an external CA or an internal CA. • External CA—An external CA organization validates identities and issues the certificates, usually for a fee. (Popular browsers are usually pre-installed with Root and Intermediate certificates issued by the external CA organization). • Internal CA—Uses a certificate-generating server within your organization (this avoids a fee). The internal CA functions exactly the same way as an external fee-based CA. This method can be used on: • Deployments that do not use HA • HA deployments that *do* use virtual IP addresses (including SSL connections between browser-based clients) **Note** Depending on your deployment, you may need to instruct your users to install the CA-signed Root and Intermediate certificates to their browser or OS certificate store. Ask your organization's IT administrator if this is required. Instructions are provided in Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 763.	Generate and Apply a CA-Signed Web Server Certificate, on page 755

Generate and Apply a CA-Signed Web Server Certificate

The following topics explain how to generate and apply CA-signed certificates to the Cisco EPN Manager web server. The procedures are slightly different depending on whether or not your deployment is using HA, and if it is using HA, whether or not you are using HA with virtual IP addresses.

You may need to instruct your users to install the Root and Intermediate CA certificates to their browser or OS certificate store. Ask your organization's IT administrator if this is required. Instructions are provided in Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 763.

Deployment Type	Summary of Steps
Deployment without HA	For deployments without HA, you must request the certificate, import it into your web server, and restart the web server to apply it, as described in these topics: **1.** Request a CA-Signed Web Server Certificate, on page 755 **2.** Import and Apply a CA-Signed Web Server Certificate—No HA, on page 756
High availability deployment *not using* virtual IP addresses	For HA deployments that do not use virtual IPs, you must request separate certificates for the primary and secondary servers and then import the appropriate certificate onto each server. When you restart the servers to apply the certificates, you must restart them in a specific order. The entire procedure is described in these topics: **1.** Request a CA-Signed Web Server Certificate, on page 755 **2.** Import and Apply CA-Signed Web Server Certificates—HA Without Virtual IP Addresses, on page 758
High availability deployment *using* virtual IP addresses	For HA deployments that use virtual IPs, you only need to request a single certificate for both servers. You must remove HA on the servers, import the certificate on both servers, and then restart the servers to apply the certificate (you must restart the servers in a specific order). Finally, you reconfigure HA by registering the secondary server on the primary server. The entire procedure is described in these topics: **1.** Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses, on page 760 **2.** How to Configure HA Between the Primary and Secondary Servers, on page 884

Request a CA-Signed Web Server Certificate

Use this procedure to request a CA-signed web server certificate for your deployment. You should use this procedure if:

- Your deployment does not use HA
- Your deployment uses HA but does not use virtual IP addressing (you will need to perform the following procedure on both servers)

Note If your deployment uses HA with virtual IP addresses, use the procedure in Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses, on page 760.

Before you begin

Make sure SCP is enabled on your machine and all relevant ports are open. This is required so that you can copy files to and from the server.

Step 1 Generate a Certificate Signing Request (CSR) file for the Cisco EPN Manager server:

a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

b) Enter the following command to generate the CSR file in the default backup repository (defaultRepo):

```
ncs key genkey -newdn -csr CertName.csr repository defaultRepo
```

where *CertName* is an arbitrary name of your choice.

Step 2 Copy the CSR file from the Cisco EPN Manager server to your local machine.

a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

b) Copy the file from the Cisco EPN Manager server to your local machine. For example:

```
scp /localdisk/defaultRepo/CertName.csr clientUserName@clientIP:/destinationFolder
```

Step 3 Submit the CSR file to a Certificate Authority of your choice.

Note Once you have generated and sent the CSR file for certification, do *not* use the **genkey** command to generate a new key on the same Cisco EPN Manager server. If you do, when you try to import the signed certificate file, you will receive an error due to a mismatch between keys in the file and on the Cisco EPN Manager server.

The CA will send you digitally-signed certificates either in a single file with the name *CertFilename***.cer**, or as a set of multiple files.

Step 4 (HA deployments not using virtual IP addresses) Repeat these steps for the secondary server.

What to do next

When your receive the certificates from the CA, import and apply the certificates. Use one of the following procedures, depending on your deployment:

- Import and Apply a CA-Signed Web Server Certificate—No HA, on page 756
- Import and Apply CA-Signed Web Server Certificates—HA Without Virtual IP Addresses, on page 758

Import and Apply a CA-Signed Web Server Certificate—No HA

This topic explains how to import and apply CA-signed web server certificates to a deployment that does not use HA.

Before you begin

- You must have the CA-signed certificates . You cannot perform the following procedure until you have received the certificates.
- Make sure SCP is enabled on your local machine and all relevant ports are open. This is required so that you can copy files to and from the server.

Step 1 If you receive only one CER file from the CA, proceed to Step 2. If you receive multiple (chain) certificates, combine (concatenate) them into a single CER file. You will receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.

a) Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This will create a file that looks like the following (the certificate contents are omitted for brevity):

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) Save this new file with a new name in the format *CertFilename*.**cer**.

Step 2 Copy the CER file from your local machine to the backup repository on the Cisco EPN Manager server.

a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

b) Retrieve the file from your local machine and copy it to the Cisco EPN Manager server default backup repository (defaultRepo):

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

Step 3 As the Cisco EPN Manager CLI admin user, import the CER file.

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

Step 4 Restart Cisco EPN Manager to activate this certificate. See Stop and Restart Cisco EPN Manager, on page 769.

What to do next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 763 for more information.

Import and Apply a CA-Signed Web Server Certificate—No HA

This topic explains how to import and apply CA-signed web server certificates to a deployment that does not use HA.

Before you begin

- You must have the CA-signed certificates . You cannot perform the following procedure until you have received the certificates.
- Make sure SCP is enabled on your local machine and all relevant ports are open. This is required so that you can copy files to and from the server.

Step 1 If you receive only one CER file from the CA, proceed to Step 2. If you receive multiple (chain) certificates, combine (concatenate) them into a single CER file. You will receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.

a) Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This will create a file that looks like the following (the certificate contents are omitted for brevity):

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) Save this new file with a new name in the format *CertFilename*.**cer**.

Step 2 Copy the CER file from your local machine to the backup repository on the Cisco EPN Manager server.

a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

b) Retrieve the file from your local machine and copy it to the Cisco EPN Manager server default backup repository (defaultRepo):

```
scp clientUserName@clientIP:/FullPathToCERfile /localdisk/defaultRepo
```

Step 3 As the Cisco EPN Manager CLI admin user, import the CER file.

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

Step 4 Restart Cisco EPN Manager to activate this certificate. See Stop and Restart Cisco EPN Manager, on page 769.

What to do next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 763 for more information.

Import and Apply CA-Signed Web Server Certificates—HA Without Virtual IP Addresses

This topic explains how to import and apply CA-signed web server certificates to an HA deployment that is *not* using virtual IP addresses. (If you have an HA deployment that *does* use virtual IPs, see Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses, on page 760.) This procedure is similar to the procedure for a deployment that does have HA, except that you have to perform the procedure on both the primary server and the secondary server.

Note When you restart the servers, follow these steps carefully because the servers must be restarted in a specific sequence.

Before you begin

- You must have the CA-signed certificates . You cannot perform the following procedure until you have received the certificates for each server.
- Make sure SCP is enabled on your local machine and all relevant ports are open. This is required so that you can copy files to and from the server.

Step 1 Import the primary certificates onto the primary server.

a) If you received only one CER file from the CA, proceed to Step 1(b). If you received multiple (chain) certificates, combine (concatenate) them into a single CER file. You will receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.

1. Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This will create a file that looks like the following (the certificate contents are omitted for brevity):

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

2. Save this new file with a new name in the format *CertFilename*.**cer**.

b) Log in to the primary Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.

c) Retrieve the CER file from your local machine and copy it to the Cisco EPN Manager server's default backup repository (defaultRepo):

```
scp clientUserName@clientIP:/fullPathToCERfile /localdisk/defaultRepo
```

Step 2 Perform the previous step on the secondary server.

Step 3 On the *secondary* server, import the CER file.

a) Log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

b) Verify that the secondary server is stopped.

c) Import the CER file:

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

Note Do not restart the secondary server until you reach Step 5.

Step 4 On the *primary* server, import the CER file.

a) Log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

b) Verify that the primary server is stopped.

c) Import the CER file:

```
ncs key importsignedcert CertFilename.cer repository RepoName
```

Note Do not restart the primary server until you reach Step 6.

Step 5 On the *secondary* server, run the following commands:

a) Run the **ncs start** command to restart the server.

b) Verify that the secondary server has restarted.

c) Run the **ncs status** command and verify that the HA status of the secondary server is **Secondary Lost Primary**.

Step 6 On the *primary* server, run the following commands:

a) Run the **ncs start** command to restart the server.

b) Verify that the primary server has restarted.

c) Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted.

Once all the processes on the primary server are up and running, HA registration is automatically triggered between the secondary and primary servers (and an email is sent to the registered email addresses). This normally completes after a few minutes.

Step 7 Verify the HA status on the primary and secondary servers by running the **ncs ha status** command on both servers. You should see the following:

- The primary server state is **Primary Active**.
- The secondary server state is **Secondary Syncing**.

What to do next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 763 for more information.

Request, Import, and Apply a CA-Signed Web Server Certificate—HA With Virtual IP Addresses

If you have a high availability deployment that uses virtual IP addresses, you need to make only one certificate request. When you receive the certificate from the CA, you install the same certificate on both the primary and secondary servers. This is different from HA deployments that do not use virtual IP addressing, where you make two certificate requests and install one certificate on the primary server and the other (different) certificate on the secondary server.

For more information on virtual IPs and HA, see Using Virtual IP Addressing With HA, on page 882

Before you begin

Make sure that SCP is enabled on your machine and all relevant ports are open. This is required so that you can copy files to and from the server.

Step 1 Generate a CSR file and private key for the primary and secondary servers. You install the private key on both servers, and submit the CSR file to a Certificate Authority of your choice. The following example shows how to create these files using openssl in Linux.

a) Generate the CSR file in the default backup repository.

```
openssl req -newkey rsa:2048 -nodes -keyout ServerKeyFileName -out CSRFileName -config
opensslCSRconfigFileName
```

where:

- *ServerKeyFileName* is the name that you want to use for the private key file.
- *CSRFileName* is the name that you want to use for the CSR request file, which will be submitted to the CA.
- *opensslCSRconfigFileName* is the name of the file that contains the openssl configurations used to generate the CSR file.

b) Using a text editor, edit the file with openssl configurations (*opensslCSRconfigFileName* in (a)) to have contents similar to the following.

```
[req]
 distinguished_name = req_distinguished_name
 req_extensions = v3_req

 [req_distinguished_name]
 countryName = Country
 countryName_default = US
 stateOrProvinceName = State
 stateOrProvinceName_default = CA
 localityName = City
 localityName_default = San Jose
 organizationName = Organization
 organizationName_default = Cisco Systems
 organizationalUnitName = Organizational Unit
 organizationalUnitName_default = CSG
 commonName = Common Name
 commonName_default = example.cisco.com
 commonName_max = 64

 [ v3_req ]
 # Extensions to add to a certificate request
 basicConstraints = CA:FALSE
 keyUsage = nonRepudiation, digitalSignature, keyEncipherment
 subjectAltName = @alt_names

 [alt_names]
 DNS.1 = example.cisco.com
 DNS.2 = example-pri.cisco.com
 DNS.3 = example-sec.cisco.com
 IP.1 = 209.165.200.224
 IP.2 = 209.165.200.225
 IP.3 = 209.165.200.226
```

In this example:

- The virtual IP address is 209.165.200.224. The FQDN for is **example.cisco.com**. The FQDN is also used for the DNS server name.
- The primary server IP address is 209.165.200.225. Its hostname is **example-pri**. This hostname should be included in /etc/hosts and other hostname setting files.
- The secondary server IP address is 209.165.200.226. Its hostname is **example-sec**.

Step 2 Submit the CSR file to a Certificate Authority of your choice. The CA sends you digitally signed certificates either in a single file with the name *CertFilename***.cer**, or as a set of multiple files.

Step 3 If you receive only one CER file from the CA, proceed to Step 4. If you receive multiple (chain) certificates, combine (concatenate) them into a single CER file. You receive three files: the SSL server certificate file, the intermediate CA certificate file, and the root CA server certificate file.

a) Using a text editor, open the three certificate files that you received. Paste the contents of the certificates into a single *new* file, from top to bottom in this order: your SSL Server certificate, the Intermediate CA certificate, and the Root CA server certificate. Remove any blank lines. This creates a file that looks like the following (the certificate contents are omitted for brevity):

```
----BEGIN CERTIFICATE-----
Your_SSL_Server_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Intermediate_CA_Cert_Contents
-----END CERTIFICATE-------
-----BEGIN CERTIFICATE-----
Root_CA_Cert_Contents
-----END CERTIFICATE-------
```

b) Save this new file with a new name in the format *CertFilename***.cer**.

Step 4 On the primary server, copy the CER file to the backup repository on each server.

a) Log in to the Cisco EPN Manager server as the Cisco EPN Manager CLI admin user.
b) Retrieve the file from your local machine and copy it to the server's default backup repository (defaultRepo).

Step 5 Repeat the previous step on the secondary server.

Step 6 On the *primary* server, as the Cisco EPN Manager CLI admin user, remove the HA settings:

```
ncs ha remove
```

Run the **ncs ha status** to verify if the HA settings are removed before proceeding with the next step.

Note If the HA is unassigned, you need to delete the TOFU certificates manually. For more information, see Resolve TOFU Failure at Any State, on page 913.

Step 7 On both the primary and secondary server, import the CER file.

```
ncs key importkey ServerKeyFileNameCertFilename.cer repository RepoName
```

Step 8 Restart the primary and secondary servers. Because they are not yet paired for HA, the order does not matter. See Stop and Restart Cisco EPN Manager, on page 769.

Note If the server does not restart, it may indicate that you mistakenly imported an individual certificate file instead of a concatenated certificate file (even though the import operation appeared to be successful). To fix this, repeat the import operation using the (correct) concatenated certificate file.

Step 9 Verify the status of the primary and secondary servers by running the **ncs status** command on both servers.

Step 10 Register the secondary server on the primary server for HA. See How to Configure HA Between the Primary and Secondary Servers, on page 884.

What to do next

Depending on your deployment, you may need to instruct your users to install the root and intermediate CA certificates to their browser or OS certificate store. See Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store, on page 763 for more information.

Add the CA-Signed Root and Intermediate Certificates to a Browser/OS Trust Store

Ask your organization's IT administrator if your users should install the CA Root and Intermediate CA certificates to their browser or OS certificate store. If not done in situations where it is required, users see indications on their browsers that the browsers are not trusted.

Depending on your browser type and version, the exact steps for this procedure may be slightly different.

Before you begin

If you are adding the certificates to a Chrome browser, you must have Administrator privileges on your client machine.

Step 1 For Firefox browsers, follow these steps to import the certificates.

a) Choose **Tools** > **Options**, then click **Advanced** from the options on the left.
b) Click **Certificates** from the list at the top of the window, then click **View Certificates**. This opens the browser's Certificate Manager dialog box.
c) In the Certificate Manager dialog box, click the **Authorities** tab, then click **Import** at the bottom of the dialog box.
d) In the **Select File...** dialog box, browse to the CA-signed Root certificate file, then click **Open**.
e) Import the file.
f) Repeat the import steps for the CA-signed Intermediate certificate file.

Step 2 For Google Chrome browsers, use the Microsoft Certificate Manager tool to import the certificates. To use this tool, users must have Administrator privileges on their client machine.

a) In Windows 7, click **Start**.
b) Enter **certmgr.msc** in the Search text box, the hit Return.
c) Launch the Microsoft Certificate Manager by clicking the program's icon in the Search results.
d) In the left column of the Certificate Manager GUI, choose **Trusted Root Certification Authorities**.
e) Left-click **Certificates**, then choose **All Tasks** > **Import**.
f) Click **Next**, then browse to the CA-signed Root certificate file, and import it.
g) Repeat the import steps for the CA-signed Intermediate certificate file, but choose **Intermediate Certification Authorities** as the first step for importing the certificate.

Note If a CA-signed certificate is not installed, then Cisco EPN Manager displays an alert.

Change the HTTPS Server Port

Because many devices use HTTPS to relay device configuration information, HTTPS is enabled by default in Cisco EPN Manager. (HTTP is not used by Cisco EPN Manager and is disabled by default.) If needed, you can change the port for the HTTPS server by following these steps.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

Step 2 In the HTTPS area, enter the new port number, then click **Save**.

Step 3 Restart Cisco EPN Manager to apply your changes. See Stop and Restart Cisco EPN Manager, on page 769.

Set Up Certificate Validation

During secure transactions like TLS/HTTPS connection, user authentication (when certificate base authentication is enabled), Cisco EPNM will receive certificates from external entities. Cisco EPNM needs to validate these certificate to ascertain the integrity of the certificate and the identity of the certificate holder. Certificate validation features allows the user to control how the certificates received from other entities are validated.

When the certificate validation is enforced, certificates received from other entities would be accepted by Cisco EPNM only if that certificate is signed by certificate authority (CA) trusted by Cisco EPNM. Trust store is where user can maintain the trusted CA certificates. If the signed certificate chain is not rooted to one of the CA certificates in the trust store, validation will fail.

Managing Trust Store

User can manage the trusted CAs in the trust store. Cisco EPNM provides different trust stores namely – pubnet, system, devicemgmt and user.

- pubnet – Used while validating certificates received from remote hosts when connecting to servers in public network.
- system – Used while validating certificates received from remote systems when connecting to systems within network.
- devicemgmt – Used while validating certificates received from managed devices.
- user – Used to validate user certificates (When certificate based authentication is enabled).

CLIs to Manage Trust Store

The following is the CLI used to manage the trsut store.

- Importing a CA certificate to Trust Store, on page 764
- Viewing a CA Certificate in a Trust Store, on page 765
- Deleting a CA certificate from a trust store, on page 765

Importing a CA certificate to Trust Store

The following is the command to import CA certificate to a trust store:

```
ncs certvalidation trusted-ca-store importcacert alias <ALIAS> repository
<Repository-name><certificate-file> truststore {devicemgmt | pubnet |
system | user}
```

Viewing a CA Certificate in a Trust Store

The following is the command to view CA certificate in a trust store:

```
ncs certvalidation trusted-ca-store listcacerts truststore {devicemgmt |
pubnet | system | user}
```

Deleting a CA certificate from a trust store

The following is the command to delete CA certificate to a trust store:

```
ncs certvalidation trusted-ca-store deletecacert alias <ALIAS> truststore
{devicemgmt | pubnet | system | user}
```

Establish an SSH Session With the Cisco EPN Manager Server

When you connect to the server, use SSH and log in as the admin user. (See User Interfaces, User Types, and How To Transition Between Them, on page 789 for more information.)

Step 1 Start your SSH session and log in as the Cisco EPN Manager admin user.

- From the command line, enter the following, where *server-ip* is the Cisco EPN Manager:

  ```
  ssh admin server-ip
  ```

- Open an SSH client and log in as **admin**.

  Note Users can now create and customize new algorithms to connect to SSH or PuTTY.

Step 2 Enter the admin password. The prompt will change to the following:

```
(admin)
```

To view a list of the operations the admin user can perform, enter **?** at the prompt.

To enter admin config mode, enter the following command (note the change in the prompt):

```
(admin) configure terminal
(config)
```

Set Up NTP on the Server

Network Time Protocol (NTP) must be properly synchronized on all devices in your network as well as on the Cisco EPN Manager server. Failure to manage NTP synchronizations across your network can result in anomalous results in Cisco EPN Manager. This includes all Cisco EPN Manager-related servers: Any remote

FTP servers that you use for Cisco EPN Manager backups, secondary Cisco EPN Manager high-availability servers, and so on.

You specify the default and secondary NTP servers during Cisco EPN Manager server installation. You can also use Cisco EPN Manager's **ntp server** command to add to or change the list of NTP servers after installation.

Note Cisco EPN Manager cannot be configured as an NTP server; it acts as an NTP client only. . You can configure up to five NTP servers.

Step 1 Log in to the Cisco EPN Manager server as the admin user and enter config mode. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Set up the NTP server using one of the following commands.

For an unauthenticated NTP server setup:

```
ntp server ntp-server-IP
```

For an authenticated NTP server setup:

```
ntp server ntp-server-IP ntp-key-id ntp-type password
```

Where:

- *ntp-server-IP* is the IP address or hostname of the server providing the clock synchronization to the Cisco EPN Manager server
- *ntp-key-id* is the md5 key ID md5 key of the authenticated NTP server
- *ntp-type* can be plain or hash
- *password* is the corresponding plain-text md5 password for the NTPv4 server

Set Up the Cisco EPN Manager Proxy Server

Use this procedure to configure proxies for the server and, if configured, its local authentication server. If you use a proxy server as a security barrier between your network and the Internet, you need to configure the proxy settings as shown in the following steps:

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Account Settings**.

Step 2 Click the **Proxy** tab.

Step 3 Select the **Enable Proxy** check box and enter the required information about the server that has connectivity to Cisco.com and will act as the proxy.

Step 4 Select the **Authentication Proxy** check box and enter the proxy server's user name and password.

Step 5 Click **Test Connectivity** to check the connection to the proxy server.

Step 6 Click **Save**.

Set Up the SMTP E-Mail Server

To enable Cisco EPN Manager to send email notifications (for alarms, jobs, reports, and so forth), the system administrator must configure a primary SMTP email server (and, preferably, a secondary email server).

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Mail and Notification** > **Mail Server Configuration**.

Step 2 Under Primary SMTP Server, complete the Hostname/IP, User Name, Password, Port, Connection Security, and Confirm Password fields as appropriate for the email server you want Cisco EPN Manager to use. Enter the IP address of the physical server. and the Enter the hostname of the primary SMTP server.

Note You cannot enter a virtual IP address in the Hostname/IP field, and the IP address cannot be behind a load balancer.

Step 3 (Optional) Complete the same fields under Secondary SMTP Server.

Step 4 Under Sender and Receivers, enter a legitimate email address for Cisco EPN Manager.

Step 5 Click **Save**.

Enable FTP/TFTP/SFTP Service on the Server

FTP/TFTP/SFTP is used to transfer files between the server and devices for device configuration and software image file management. These protocols are also used in high availability deployments to transfer files to a secondary server. These services are normally enabled by default. If you installed Cisco EPN Manager in FIPS mode, they are disabled by default. If you use this page to enable these services, Cisco EPN Manager will become non-compliant with FIPS.

SFTP is the secure version of the file transfer service and is used by default. FTP is the unsecured version of the file transfer service; TFTP is the simple, unsecured version of the service. If you want to use either FTP or TFTP, you must enable the service after adding the server.

To change the FTP/TFTP/SFTP password, see Change the FTP User Password, on page 770.

Step 1 Configure Cisco EPN Manager to use the FTP, TFTP, or SFTP server.

a) Choose **Administration** > **Servers** > **TFTP/FTP/SFTP Servers**.

b) From the **Select a command** drop-down list, choose **Add TFTP/FTP/SFTP Server**, then click **Go**.

- From the **Server Type** drop-down list, choose **FTP**, **TFTP**, **SFTP**, or **All**.
- Enter a user-defined name for the server.
- Enter the IP address of the server.

c) Click **Save**.

Step 2 If you want to use FTP or TFTP, enable it on the Cisco EPN Manager server.

a) Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

b) Go to the FTP or TFTP area.

c) Click **Enable**.
d) Click **Save**.

Step 3 Restart Cisco EPN Manager to apply your changes. See Stop and Restart Cisco EPN Manager, on page 769.

Note In a High Availability setup, in case the FTP or TFTP services are enabled in the primary server, they must also be enabled in the secondary server before High Availability is configured. This must be done manually on the secondary server by editing a configuration file and restarting the server in order to apply the change.

Below are the steps which must be performed on the secondary server:

- To Enable FTP or TFTP on the secondary server
  1. Set the following properties to value "**true**" in file `/opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml`
     - <entry key="FtpEnable">true</entry>
     - <entry key="TftpEnable">true</entry>
  2. Restart Cisco EPN Manager secondary server.
- To Disable FTP or TFTP on the secondary server
  1. Set the following properties to value "**false**" in file `/opt/CSCOlumos/conf/rfm/classes/com/cisco/packaging/PortResources.xml`
     - <entry key="FtpEnable">false</entry>
     - <entry key="TftpEnable">false</entry>
  2. Restart Cisco EPN Manager secondary server.

Create a Login Banner (Login Disclaimer)

When you have a message that you want to display to all users before they log in, create a login disclaimer. The text will be displayed on the GUI client login page below the login and password fields.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Login Disclaimer**.

Step 2 Enter (or edit) the login disclaimer text.

Note Carriage returns are ignored.

Your changes will take effect immediately.

Stop and Restart Cisco EPN Manager

A Cisco EPN Manager restart is needed in cases such as after a product software upgrade, log file setting changes, hanging secure port settings, compressing report files, changing service discovery settings, and, configuring LDAP settings. When you stop the Cisco EPN Manager server, all user sessions are terminated.

To stop the server, open a CLI session with the server and enter:

```
ncs stop
```

To restart the server, open a CLI session with the server and enter:

```
ncs start
```

Configure Global SNMP Settings for Communication with Network Elements

The SNMP Settings page controls the how the server uses SNMP to reach and monitor devices. These settings determine when a device is considered unreachable. Any changes you make on this page are applied globally and are saved across restarts, backups, and restores.

Note The default network address is 0.0.0.0, which indicates the entire network. An SNMP credential is defined per network, so only network addresses are allowed. 0.0.0.0 is the default SNMP credential and is used when no specific SNMP credential is defined. You must update the prepopulated SNMP credential with your own SNMP information.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Network and Device** > **SNMP**.

Step 2 Choose an algorithm from the **Backoff Algorithm** drop-down list.

- **Exponential**—Each SNMP try waits twice as long as the previous try, starting with the specified timeout for the first try.
- **Constant Timeout**—Each SNMP try waits the same amount of time (timeout). This is useful on unreliable networks where the desired number of retries is large. Because it does not double the timeout per try, it does not take as long to timeout with a high number of retries.

Step 3 Select the **Use Reachability Parameters** checkbox to configure global **Reachability Retries** and **Reachability Timeout** values. Selecting this option will cause Cisco EPN Manager to default to the values configured here.

Note If the **Use Reachability Parameters** check box is not selected, Cisco EPN Manager uses the timeout and retries specified by the device.

- **Reachability Retries** — Enter the number of global retries to determine device reachability.

  You can edit this field only if the **Use Reachability Parameters** checkbox is selected. If switch port tracing is taking a longer to complete, reduce the **Reachability Retries** value.

- **Reachability Timeout** — The default value is 2 seconds. You cannot edit this field.

Step 4 In the **Maximum VarBinds per Get PDU** and **Maximum VarBinds per Set PDU** fields, enter a number to indicate the largest number of SNMP variable bindings allowed in a request or response PDU. These fields enable you to make necessary changes when you have any failures associated to SNMP. For customers who have issues with PDU fragmentation in their network, the number can be reduced to 50, which typically eliminates the fragmentation.

Step 5 Optionally adjust the **Maximum Rows per Table**.

Step 6 Click **Save**.

Manage Administrative Passwords

Change the FTP User Password

Cisco EPN Manager uses the ID **ftp-user** to access other servers using FTP. Users with Admin privileges can change the FTP password.

Step 1 Log in to the Cisco EPN Manager server as the admin user. Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 To change the Cisco EPN Manager server's FTP password, enter:

```
ncs password ftpuser username password password
```

Example

```
(admin) ncs password ftpuser ftp-user password FTPUserPassword
Initializing...
Updating FTP password.
This may take a few minutes.
Successfully updated location ftpuser
```

Change the Web GUI Root User Password

Cisco EPN Manager uses the **root** ID to perform special tasks that require root access to the web GUI.

Before you begin

You must know the current web GUI root user password to change it.

Step 1 Log in to the Cisco EPN Manager Admin CLI as the **root** user. (For information on the Admin CLI, see User Interfaces and User Types, on page 789.)

Step 2 Enter the following command, where *newpassword* is the new web GUI root password:

```
ncs password root password  newpassword
```

Note The new password you enter must adhere to the current password policies. For more information, see Configure Global Password Policies for Local Authentication, on page 813.

Example

```
ncs password root password NewWebGUIRootPassword
Password updated for web root password
```

Recovering Administrator Passwords on Virtual Appliances

This topic explains how to recover and reset the admin password on Cisco EPN Manager virtual machines (also known as OVAs).

Before You Begin

Ensure that you have:

- Physical access to the Cisco EPN Manager server.
- A copy of the installation ISO image appropriate for your version of the software.
- Access to the VMware vSphere client, and to the vSphere inventory, Datastores and Objects functions. If you do not have such access, consult your VMware administrator. Avoid accessing ESX directly from the vSphere client.

Step 1 At the Cisco EPN Manager OVA server, launch the VMware vSphere client.

Step 2 Upload the installation ISO image to the data store on the OVA virtual machine, as follows:

a) In the vSphere inventory, click **Datastores**.
b) On the **Objects** tab, select the datastore to which you will upload the file.
c) Click the **Navigate to the datastore file browser** icon.
d) If needed, click the **Create a new folder** icon and create a new folder.
e) Select the folder that you created or select an existing folder, and click the **Upload a File** icon.

   If the Client Integration Access Control dialog box appears, click **Allow** to allow the plug-in to access your operating system and proceed with the file upload.

f) On the local computer, find the ISO file and upload it.
g) Refresh the datastore file browser to see the uploaded file in the list.

Step 3 With the ISO image uploaded to a datastore, make it the default boot image, as follows:

a) Using the VMware vSphere client, right-click the deployed OVA and choose **Power > Shut down guest**.
b) Select **Edit Settings > Hardware**, then select **CD/DVD drive 1**.
c) Under **Device Type**, select **Datastore ISO File**, then use the **Browse** button to select the ISO image file you uploaded to the datastore.
d) Under **Device Status,** select **Connect at power on**.
e) Click the **Options** tab and select **Boot Options**. Under **Force BIOS Setup**, select **Next time VM boots, force entry into BIOS setup Screen**. This will force a boot from the virtual machine BIOS when you restart the virtual machine.
f) Click **OK**.
g) In the VMware vSphere client, right-click the deployed OVA and choose **Power > Power On**.
h) In the BIOS setup menu, find the option that controls the boot order of devices and move **DVD/CDROM** to the top.

Step 4 Follow the steps below to reset a server administrator password:

a) Save your BIOS settings and exit the BIOS setup menu. The virtual machine will boot from the ISO image and display a list of boot options.
b) Enter **3** if you are using the keyboard and monitor to access the OVA, or **4** if you are accessing via command line or console. The vSphere client displays a list of administrator user names.
c) Enter the number shown next to the administrator username for which you want to reset the password.
d) Enter the new password and verify it with a second entry.
e) Enter **Y** to save your changes and reboot.
f) Once the virtual machine has rebooted: Using the vSphere client, click on the CD icon and select **Disconnect ISO image**.

Step 5 Log in with the new admin password.

Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard

The System Monitoring Dashboard provides information about the configuration and performance of the Cisco EPN Manager server. To access the dashboard, choose **Administration** > **Dashboards** > **System Monitoring Dashboard** (your User ID must have administrator privileges to access this dashboard). If you want to customize the dashlets that are displayed in the Overview or Performance tabs, follow the instructions in Add a Predefined Dashlet To a Dashboard, on page 21.

Dashboard Tab	Description
Overview	Backup and data purging jobs, Cisco EPN Manager system alarms, and utilization statistics for server CPU, disk, and memory. You can specify different time frames to check this information. To view the server time, kernel version, operating system, hardware information, and so forth, click **System Information** at the top left of the dashboard to open a field with that information. You can add and delete dashlets from the Overview dashboard.
Performance	Server syslogs and traps, and input/output. You can specify different time frames for this data, and add and remove dashlets from the Performance dashboard.
Admin	• Health—System alarms, number of jobs running, number of users logged in, and database usage distribution. You can specify different time frames for historical information. • API Health—Lists all API services with their response time statistics. • Service Details—Statistics for a specific service (response count and time trend, calls per client (clients are identified by their IP address). You can pick the service you want to check.

Improve the Cisco EPN Manager Server Performance

Check the OVA Size

If Cisco EPN Manager is using 80 percent or more of your system resources or the device/interface/flow counts recommended for the size of OVA you have installed, this can negatively impact performance. Make sure the OVA is not exceeding the device, interface, and flow record recommendations given in the installation documentation. They are the maximums for each given OVA size. You can check these from the Admin Dashboard (see Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard, on page 772). To respond to space issues, see Manage Server Disk Space Issues, on page 773.

Compact the Database

Step 1 Log in to the server as the admin user. Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter the following command to compact the application database:

```
(admin)# ncs cleanup
```

Step 3 When prompted, answer **Yes** to the deep cleanup option.

Manage Server Disk Space Issues

Cisco EPN Manager will trigger alarms indicating that the server is low on disk space at the following thresholds:

- 60% usage triggers a Major alarm
- 65% usage triggers a Critical alarm

If you receive an alert, consider performing the following actions:

- Free up existing database space as explained in Compact the Database, on page 773.
- If you are saving backups to a local repository, consider using a remote backup repository. See Set Up NFS-Based Remote Repositories, on page 738.
- Reduce the retention period for network inventory, performance, reports, and other classes of data as explained in Data Collection and Purging, on page 781.
- Add more disk space. VMware OVA technology enables you to easily add disk space to an existing server. You will need to shut down the Cisco EPN Manager server and then follow the instructions provided by VMware to expand the physical disk space. Once you restart the virtual appliance, Cisco

EPN Manager automatically makes use of the additional disk space (see Data Collection and Purging, on page 781).

- Set up a new server that meets at least the minimum RAM, disk space, and processor requirements of the next higher level of OVA. Back up your existing system, then restore it to a virtual machine on the higher-rated server.

Configure Network Team (Link Aggregation)

With Cisco EPN Manager, you can create NIC teaming to maintain redundancy. It enables you to bind up to 256 physical interfaces into one logical interface with a single IP address. This means that the connection is not interrupted even if one of the interfaces goes down. You can perform regular interface operations on the logical interface.

Note Teaming is not supported for Eth 0 / Gigabitethernet 0 port which is used for NBI.

Step 1 Log into the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter configuration mode:

```
configure terminal
config#
```

Step 3 Configure the logical interface, then exit configuration mode:

```
config# interface interfaceName
config-InterfaceName# ip addressIP_addresssubnet_mask
config-InterfaceName# member interface1
config-InterfaceName# member interface2
config-InterfaceName# exit
config# exit
```

Where:

- *interfaceName* is the name of the logical interface (for example, Team0).
- *IP_address*, *subnet_mask* the IP address and subnet mask you want to assign to the logical interface.
- *interface1* , *interface2* are the names of the physical interfaces you want to bind into your logical interface(for example GigabitEthernet 1, GigabitEthernet 2)

Step 4 Verify the creation of the logical interface:

```
show interface interfaceName
```

Create or Modify an IP Access-List to Filter Network Traffic

Cisco EPN Manager maintains a pre-configured default IP access-list named *default*. This list cannot be modified, but you can be assign or un-assign it to NICs.

You can create or modify a new IP access-list to filter ingress network traffic to Cisco EPN Manager. The default behavior is to block network traffic unless it is explicitly specified in the IP access list. To create a new IP access list:

Step 1 Log into the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter configuration mode:

```
configure terminal
config#
```

Step 3 Create an ip access-list specifying the port and protocol information, then exit the configuration mode.

```
config-InterfaceName# ip access-list listname
config-ACL-listname# permit protocol1 port1
config-ACL-listname# permit protocol2 port2
config-ACL-listname# exit
config# exit
```

Where:

- *listname* - name of the new IP access-list (for example, test_acl).
- **permit** - command to add protocols and ports information to route the network traffic.

Note Use the no form of the permit command if you want block specific kind of network traffic through a port.

Step 4 4. To view the newly created IP access-list, use

```
show running-config
```

Assign a IP Access-list to an Interface

Follow this procedure to assign a IP access-list to an interface. If an access-group (list) is already assigned to a NIC and you assign a new one, Cisco EPN Manager replaces the older list with the new one.

Important To use different access-lists for different interfaces, ensure that the IP addresses assigned to the interfaces are NOT in the same network / subnet.

Step 1 Log into the server as the Cisco EPN Manager CLI admin user. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

Step 2 Enter configuration mode:

```
configure terminal
config#
```

Step 3 3. Assign the IP access-list to the interface.

```
config# interface interfaceName
config-InterfaceName# ip access-group acl_name  in
config-InterfaceName# exit
config# exit
```

Where:

- *interfaceName* - name of the interface.
- **ip access-group** - command to add the IP access-list to the interface.
- *acl_name* - IP access-list that is to be assigned to the interface.
- **in** - for ingress.

Note Currently, this is the only supported direction.

Step 4 4. Verify if the access list has been assigned to the device.

```
show running-config
```

Example

```
config# interface GigabitEthernet 0
config-GigabitEthernet-0# ip access-group test_acl
```

Work With Server Internal SNMP Traps That Indicate System Problems

Cisco EPN Manager generates internal SNMP traps that indicate potential problems with system components. This includes hardware component failures, high availability state changes, backup status, and so forth. The failure trap is generated as soon as the failure or state change is detected, and a clearing trap is generated if the failure corrects itself. For TCAs (high CPU, memory and disk utilization traps, and so forth), the trap is generated when the threshold is exceeded.

A complete list of server internal SNMP traps is provided in . Cisco EPN Manager sends traps to notification destination on port 162. This port cannot be customized at present.

You can customize and manage these traps as described in the following topics:

- Customize Server Internal SNMP Traps and Forward the Traps, on page 777
- Troubleshoot Server Internal SNMP Traps, on page 777

Customize Server Internal SNMP Traps and Forward the Traps

You can customize server internal SNMP traps by adjusting their severity or (for TCAs) thresholds. You can also disable and enable the traps. You can find the server internal SNMP traps listed in *Cisco Evolved Programmable Network Manager Supported Alarms*.

Note Cisco EPN Manager does not send SNMPv2 Inform or SNMPv3 notifications.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **System Event Configuration**.

Step 2 For each SNMP event you want to configure:

a) Click on the row for that event.

b) Set the **Event Severity** to Critical, Major, or Minor, as needed.

c) For the CPU, disk, memory utilization, and other hardware traps, Enter the **Threshold** percentage (from 1–99). These events will send the associated SNMP traps when the utilization exceeds the threshold limit. (You cannot set thresholds for events for which the threshold setting is shown as NA.) These events send traps whenever the associated failure is detected.

d) For the **EPNM User Sessions** event, enter the**Threshold** value between 1 and 150. The default value of this threshold is 5.

e) For backup threshold and certificate expiry (critical), enter the **Threshold** in days (from *x*–*y*, where *x* is the minimum number of days and *y* is the maximum number of days).

f) To control whether a trap is to generated or not, set the **Event Status**.

Step 3 In the **Other Settings**, enter the desired value for **Create and Clear Alarm Iteration**.

Step 4 To save all of your trap changes, click **Save** (below the table).

Step 5 To view the latest list of alarms and events, choose **Monitor** > **Monitoring Tools** > **Alarms and Events**.

Step 6 If you want to configure receivers for the server internal SNMP traps, refer to the procedures in the following topics, see Configure Alarms Notification Destination, on page 843.

Troubleshoot Server Internal SNMP Traps

Cisco EPN Manager provides a complete list of server internal SNMP traps, their probable cause, and recommended actions to remedy the problem. If that document does not provide the information you need, follow this procedure to troubleshoot and get more information about Cisco EPN Manager server issues.

Step 1 Ping the notification receiver from the Cisco EPN Manager server to ensure that there is connectivity between Cisco EPN Manager and your management application.

Step 2 Check if any firewall ACL settings are blocking port 162, and open communications on that port if needed.

Step 3 Log in to Cisco EPN Manager with a user ID that has Administrator privileges. Select **Administration** > **Settings** > **Logging** > **Global Settings** tab and download the log files. Then compare the activity recorded in these log files with the activity that you are seeing in your management application:

- ncs_nbi.log: This is the log of all the northbound SNMP trap messages Cisco EPN Manager has sent. Check for messages you have not received.

- ncs-# -# .log: This is the log of most other recent Cisco EPN Manager activity. Check for hardware trap messages you have not received.
- hm-# -# .log: This is the log of all Health Monitor activity. Check for recent messages about High Availability state-changes and application-process failures that you have not received.

The messages you see that in these logs should match the activity you see in your management application. If you find major differences, open a support case with Cisco Technical Assistance Center (TAC) and attach the suspect log files with your case. See Open a Cisco Support Case, on page 861.

Set Up Defaults for Cisco Support Requests

By default, users can create Cisco support requests from different parts of the Cisco EPN Manager GUI. If desired, you can configure the sender e-mail address and other e-mail characteristics. If you do not configure them, users can supply the information when they open a case.

If you do not want to allow users to create requests from the GUI client, you can disable that feature.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Account Settings**.

Step 2 Click the **Support Request** tab.

Step 3 Select the type of interaction you prefer:

- Enable interactions directly from the server—Specify this option to create the support case directly from the Cisco EPN Manager server. E-Mails to the support provider are sent from the e-mail address associated with the Cisco EPN Manager server or the e-mail address you specify.
- Interactions via client system only—Specify this option to download the information required for your support case to a client machine. You must then e-mail the downloaded support case details and information to the support provider.

Step 4 Select your technical support provider:

- Click **Cisco** to open a support case with Cisco Technical Support, enter your Cisco.com credentials, then click **Test Connectivity** to check the connectivity to the following servers:
  - Cisco EPN Manager mail server
  - Cisco support server
  - Forum server
- Click **Third-party Support Provider** to create a service request with a third-party support provider. Enter the provider's e-mail address, the subject line, and the website URL.

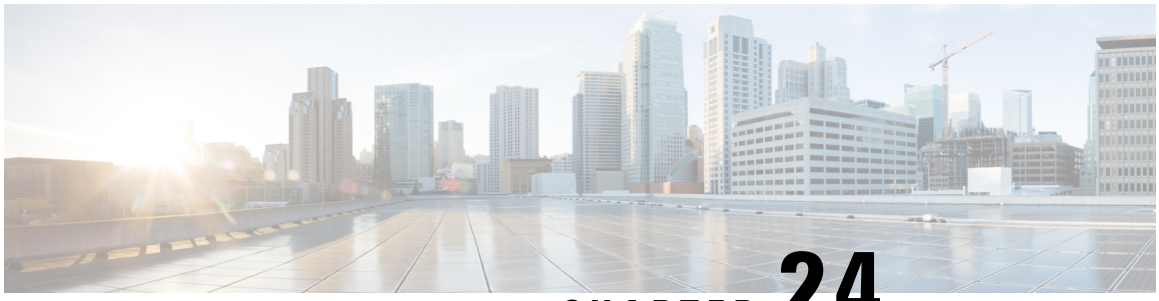
Monitor Backups

Use this procedure to view Cisco EPN Manager backup information such as file name, size, available size, and data.

Step 1 Choose **Administration** > **Dashboards** > **System Monitoring Dashboard**.

Step 2 Click the **Overview** tab. The **Backup Information** dashlet is displayed here.

Note Information in the backup dashlet is available only when the backup repository is local.



CHAPTER 24

Data Collection and Purging

Control Data Collection Jobs

All data collection tasks (and data purging tasks) are controlled from the Jobs Dashboard. See Manage Jobs Using the Jobs Dashboard, on page 23. Data collection jobs are listed under System Jobs .

System Jobs

The background data collection jobs that are performed by Cisco EPN Manager are listed under System Jobs. To view the System Jobs, choose **Administration** > **Dashboards** > **Job Dashboard** > **System Jobs**. From here, you can see if a job is successful, partially successful, or failed. You can also edit, run, or pause a job. To know more about managing jobs, see

To edit the job schedule:

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard** > **System Jobs**.

Step 2 Select the required job. For example, **Device Config Backup-External** under the **Infrastructure jobs** .

Step 3 Click **Edit Schedule**. In the Schedule window, select the **Start Time** and choose the **Recurrence** interval.

Step 4 Click **Submit** to save.

You can also run a job or pause a job by clicking **Run** and **Pause Series** tabs, respectively.

The following table provides information about a few data collection jobs available under the System Jobs.

Table 56: Inventory Data Collection Jobs

Task Name	Default Schedule	Description	Editable options
Infrastructure jobs			
Device Config Backup-External	15 minutes	This Job will Export all device configs (Text-Files in a Zip) to a predefined external repository. You can configure or create the repository using CLI commands and the supported repositories are FTP, SSH FTP (SFTP) and Network File System (NFS).	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job. Click the edit icon, and check the **Export only Latest Configuration** check box, to transfer only the latest configuration. You can edit the job properties based on the user permission set in Role-Based Access Control (RBAC).
Index search Entities	3 hours	This Job schedules the Index Search Entities.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Server Backup	1 day	This job schedules automatic Cisco EPN Manager server backups. The backups created are application backups.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Smart License Compliance Status	Disabled	This job runs for Smart License for the default schedule.	Non-Editable.
Inventory and Discovery Jobs			
Switch Inventory	1 day	This job collects inventory for discovered devices which are reachable periodically as per given schedule.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Failed Feature Sync	30 minutes	This job collects inventory for the only failed features for devices in CWW and does a full sync for devices CF periodically, this job is suspended by default. You can enable it based on their choice.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Status Jobs			

Task Name	Default Schedule	Description	Editable options
Autonomous AP Operational Status	5 minutes	This job schedules status polling of autonomous wireless access points.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Switch Operational Status	5 minutes	This job checks for the node reachability.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Third-Party Access Point Operational Status	3 hours	This job schedules operational status polling of third-party APs.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Third-Party Controller Operational Status	3 hours	This job schedules operational status polling of third-party Controllers.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.
Wireless AP Discovery	5 minutes	This job schedules Wireless AP discovery.	Select **Edit Schedule** > **Recurrence** and select the appropriate settings to schedule the job.

How Data Retention Settings Affect Web GUI Data

Changes you make on the Data Retention page determine the information that is displayed in the web GUI. You can open the data retention page by choosing **Administration** > **Settings** > **System Settings**, then choosing **General** > **Data Retention**.

For example, if you do not need any historical performance data older than 7 days, you can modify the performance data retention values as follows:

- Short-term Data Retention Period—1 day
- Medium-term Data Retention Period—3 days
- Long-term Data Retention Period—7 days

If you specify these settings, all data displayed in performance reports and on performance dashboards will be for the previous 7 days only. When you generate a performance report, even if you select a reporting period longer than the last 7 days, the report will contain data from the last 7 days only (because that is all of the data you selected to retain).

Similarly, if you view a performance dashboard and select a time frame longer than one week, the dashboard will contain date from the last 7 days only.

When you create the monitoring policy for interfaces, you can define the polling interval for every 15 minutes or every 5 minutes or every 1 minute. According to the selected polling interval, the device data is polled and stored in Oracle Database. The data is aggregated every 1 hour into the AHxxx table; once a day into the ADxxx table irrespective of the polling interval is set to1/5/15 minutes.

In the Interface Health Policy tab, if the frequency is set at 5 mins, you can view 12 samples for each hour. Every hour the data moves to the aggregated table and an average or mean interface statistics is calculated , and there will be one entry in the hourly aggregated table. The aggregation is the same for all the policies no matter what the polling interval is.

You can view data retention details and the age of the data storage, the event time in milliseconds and for each database the entity ID and the event time.View the performance data and aggregate data in the Performance Dashlet, > Interfaces > Traffic Utilization tab.

Performance and System Health Data Retention

Note Cisco recommends you do not change the retention periods for trend, device health, system health, and performance data because the default settings are optimized to get the most helpful information from interactive graphs.

The following table describes the information shown on the Data Retention page.

Type of Data	Description	Default Retention Settings	Retention Settings Range
Trend Data Retain Periods	Device-related historical information. Trend data is gathered as a whole and summarized as minimums, maximums, or averages.	Hourly data retain period: 15 (days) Daily data retain period: 90 (days) Weekly data retain period: 54 (weeks)	Hourly data: 1 to 31 (days) Daily data: 7 to 365 (days) Weekly data: 2 to 108 (weeks)
Device Health Data Retain Periods	SNMP-polled device data such as device reachability, and utilization for CPU, memory, and interfaces.	Hourly data retain period: 15 (days) Daily data retain period: 90 (days) Weekly data retain period: 54 (weeks)	Hourly data: 1 to 31 (days) Daily data: 7 to 365 (days) Weekly data: 2 to 108 (weeks)

Type of Data	Description	Default Retention Settings	Retention Settings Range
Performance Data Retain Periods	Assurance data such as traffic statistics. • Short-term data is aggregated every 5 minutes. • Medium-term data is aggregated every hour. • Long-term is aggregated daily. **Note** You can click **Advanced Settings** to configure the **Age (In days)** and **Max Records** of the available attributes.	Short term data retain period: 7 (days) Medium term data retain period: 31 (days) Long term data retain period: 378 (days)	Short term range: 1 to 31 (days) Medium term range: 7 to 365 (days) Long term range: 2 to 756 (days)
User Job Data Retain Period	All records for the user jobs in the completed state.	User job data retain period: 7 (days)	2 to 365 (days)
System Health Data Retain Periods	Includes most data shown on the Admin dashboards	Hourly data retain period: 1 (days) Daily data retain period: 7 (days) Weekly data retain period: 54 (weeks)	Hourly data range: 1 to 31 (days) Daily data range: 7 to 365 (days) Weekly data range: 2 to 108 (weeks)

For example, these are the retention settings for optical performance data:

- Optical 30 seconds performance data (short-term) is saved for 1 hour.
- Optical 15-minute performance data (short-term) is saved for one day by default. You can vary it 1–14 days.
- Optical 1-day performance data (medium-term) is saved for 30 days by default. You can vary it 30–90 days.

Specifying Data Retention By Database Table

Administrators can use the “Other Data Retention Criteria” section of the Data Retention page to configure retention periods for specific Cisco EPN Manager database tables. You specify the retention period using the following attributes:

- **Age (in hours)** : Specifies the maximum data retention period in hours for all records in the database.
- **Max Records** : Specifies the maximum number of records to retain in a particular database table. A Max Records value of NA means that the only retention criteria considered is the Age attribute.

The section is categorized into multiple subsections. Each subsection list each database table name, along with the current Age and Max Records used to determine whether an individual record in the table will be retained or discarded. The page also lists the table Age Attribute used to compute the age of the data in the table.

Cisco strongly recommends that you consult with Cisco Technical Assistance Center before changing the values for any of the tables in this section. Doing so without help may affect system performance negatively.

Step 1 Choose **Administration** > **Settings** > **System Settings** > **General** > **Data Retention**.

Step 2 Expand the **Other Data Retention Criteria** section.

Step 3 Expand the database table subsection for which you want to specify Age and Max Records values.

Step 4 Click on the database table listing and enter the new values as needed.

Step 5 Click **Save**.

Alarm, Event, and Syslog Purging

Note These default purging settings are provided to ensure optimal performance. Use care when adjusting these settings, especially if Cisco EPN Manager is managing a very large network (where increasing these settings may have an adverse impact).

Cisco EPN Manager stores a maximum of 8,000,000 events and 2,000,000 syslogs in the database.

To protect system performance, Cisco EPN Manager purges alarms, events, and syslogs according to the settings in the following table. All of these settings are enabled by default. Data is deleted on a daily basis. Alarm tables are checked hourly, and if the alarm table exceeds the 300,000 limit, Cisco EPN Manager deletes the oldest cleared alarms until the alarms table size is within the limit.

Data Type	Deleted after:	Default Setting
Alarms—Cleared security alarms	30 days	Enabled
Alarms—Cleared non-security alarms	7 days	Enabled
Events	60 days	Enabled
Syslogs	30 days	Enabled
Alarms	30 days	Disabled

To change the settings, choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarms and Events** and modify the settings in the Alarm and Event Cleanup Options area.

Log Purging

You can adjust the purging settings for logs by navigating to **Administration** > **Settings** > **Logging**. Logs are saved until they reach the maximum size. At that point, a number is appended to the log file and a new log is started. When the number of logs exceeds the maximum, the oldest log is deleted.

The **Console Log** (console.log) is managed independently and its values are not determined by the values set under **Log File Settings**. For Console Log, the default values are:

- Maximum File Size (MB): 5 MB
- Number of Files: 3

The following table lists the default purging values for General and SNMP logs.

Log Type	Size of Logs	Number of Logs	To change the setting, see:
General	10 MB	10	Adjust General Log File Settings and Default Sizes, on page 866
SNMP	10 MB	5	View and Manage General System Logs, on page 866

Report Purging

By default, reports stored in the repositories are deleted after 7 days.

The directory paths for the repositories are:

- **Scheduled Reports Repository** - /localdisk/ftp/reports
- **Ondemand Reports Repository** - localdisk/ftp/reportsOnDemand

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Report**.

Step 2 If required, adjust the location for the reports repository on the server. The repository must reside under the FTP root partition.

Step 3 If you want to change the default purging age, update the **File Retain Period** field with a value in the range 1–366 days. The default retention period is 7 days.

Step 4 Click **Save**.

Once you've updated the retention period, Cisco EPN Manager doesn’t purge the reports immediately and does so only after one night.

Backup Purging

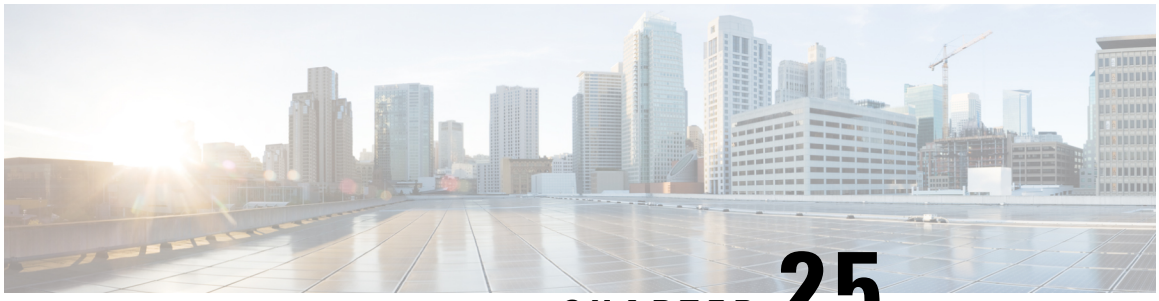
By default, 2 backups are saved for backups in local repositories. If you are using remote repositories, there is no automatic backup purging mechanism; you must manually delete old backups. See Change the Number of Automatic Application Backups That Are Saved, on page 744.

Device Configuration File Purging

For each device, 5 configuration files are saved in the configuration archive. Any file that is older than 30 days is purged. Device configuration files cannot be manually deleted.

Software Image File Purging

Device software image files are not automatically purged from the database. They must be manually removed using the GUI client. For more information, see Delete Software Image Files from the Image Repository, on page 149.



CHAPTER 25

User Permissions and Device Access

User Interfaces, User Types, and How To Transition Between Them

These topics describe the GUI and CLI interfaces used by Cisco Evolved Programmable Network Manager, and how to transition between the Cisco Evolved Programmable Network Manager and Linux CLI interfaces.

User Interfaces and User Types

The following table describes the user interfaces employed by Cisco EPN Manager, and the types of users that can access each interface.

Cisco EPN Manager User Interface	Interface Description	CEPNM User Types
Cisco EPN Manager web GUI	Web interface that facilitates day-to-day and administration operations using the web GUI. These users can have varying degrees of privileges and are classified into role-based access control (RBAC) classes and subclasses. This interface provides a subset of operations that are provided by the Cisco EPN Manager CLI admin and CLI config users.	**Cisco Evolved Programmable Network Manager web GUI everyday users**—Created by web GUI root user. These users have varying degrees of privileges and are classified into role-based access control (RBAC) classes and subclasses called *user groups* (Admin, Super Users, Config Managers, and so forth). For information on the user groups, see Types of User Groups, on page 793. **Cisco Evolved Programmable Network Manager web GUI root user**—Created at installation and intended for first-time login to the web GUI, and for creating other user accounts. This account should be disabled after creating at least one web GUI user that has Admin privileges, that is, a web GUI user that belongs to the Admin or Super Users user group. See Disable and Enable the Web GUI root User, on page 792. **Note** The Cisco EPN Manager web GUI root user is not the same as the Linux CLI root user, nor is it the same as the Cisco EPN Manager CLI admin user.
North Bound Interface (NBI) REST API	NBI is REST Application Programming Interface that allows a client system to talk to Cisco EPN Manager to carry out day-to-day and administration operations. Special privileged service account users are assigned to a client system to allow talking to Cisco EPN Manager using this interface. These NBI users can also have varying degrees of privileges and are also classified into role-based access control (RBAC) classes and subclasses.	Cisco EPN Manager NBI users—Created by web GUI root user. These users have three different types of privileges and are classified into role-based access control (RBAC) classes and subclasses called NBI user groups (NBI Read and NBI Write). For information on the user groups, see section User Groups—NBI, on page 794

Cisco EPN Manager User Interface	Interface Description	CEPNM User Types
CEPNM Admin CLI	Cisco proprietary shell which provides secure and restricted access to the system (as compared with the Linux shell). This Admin shell and CLI provide commands for advanced Cisco EPN Manager administration tasks. These commands are explained throughout this guide. To use this CLI, you must have Cisco EPN Manager CLI admin user access. You can access this shell from a remote computer using SSH.	**Cisco EPN Manager CLI Admin user**—Created at installation time and used for administration operations such as stopping and restarting the application and creating remote backup repositories. (A subset of these administration operations is available in the web GUI.) To display a list of operations this user can perform, enter **?** at the prompt. Some tasks must be performed in config mode. To transition to config mode, use the procedure in Transition Between the Cisco Evolved Programmable Network Manager admin CLI and Cisco Evolved Programmable Network Manager config CLI, on page 791. The admin CLI user can create other CLI users for various reasons, using the following command: `(config) username username password role {admin|user} password` These users may have admin-like privilege/roles or lower-level privileges as defined during creation time. To create a Cisco Evolved Programmable Network Manager CLI user with admin privileges, run the **username** command with the **admin** keyword; otherwise, use the **user** keyword. For password limitations, see Create Admin User, on page 725.
CEPNM Config CLI	Cisco proprietary shell which is restricted and more secure than the Linux shell. This Config shell and CLI provide commands for Cisco EPN Manager system configuration tasks. These commands are explained throughout this guide. To use this CLI, you must have admin-level user access (see the information in the User Types column of this table). You can access this shell in the Admin CLI shell.	
Linux CLI	Linux shell which provides all Linux commands. The Linux shell should only be used by Cisco technical support representatives. Regular system administrators should not use the Linux shell. You cannot reach this shell from a remote computer using SSH; you can only reach it through the admin shell and CLI.	**Linux CLI admin user**—Created at installation time and used for Linux-level administration purposes.

How to Transition Between the CLI User Interfaces in Cisco Evolved Programmable Network Manager

Refer to the following section to understand how to transition between the Cisco EPN Manager admin CLI and Cisco EPN Manager config CLI

Transition Between the Cisco Evolved Programmable Network Manager admin CLI and Cisco Evolved Programmable Network Manager config CLI

To move from the Cisco Evolved Programmable Network Manager admin CLI to the Cisco Evolved Programmable Network Manager config CLI, enter **config** at the admin prompt.

```
(admin)# config
(config)#
```

To move from the config CLI back to the admin CLI, enter **exit** or **end** at the config prompt:

```
(config)# exit
(admin)#
```

Enable and Disable root Access for the Cisco EPN Manager Web GUI

After installation, you should disable the Cisco EPN Manager web GUI **root** user after creating at least one other web GUI user that has Admin or Super Users privileges. See Disable and Enable the Web GUI root User, on page 792.

Disable and Enable the Web GUI root User

Step 1 Log into the Cisco EPN Manager web GUI as root, and create another web GUI user that has root privileges—that is, a web GUI user that belongs to the Admin or Super Users user group. Once this is done, you can disable the web GUI **root** account.

Step 2 Disable the Cisco EPN Manager web GUI root user account. (The web GUI admin account, which remains active, can perform all required CLI functions.)

```
ncs webroot disable
```

Step 3 To re-enable the account:

```
ncs webroot enable
```

Control the Tasks Web Interface Users Can Perform

For Web Interface users, in Cisco EPN Manager user authorization is implemented through user groups. A user group contains a list of tasks that control which parts of Cisco EPN Manager a user can access and the tasks the user can perform in those parts.

While user groups control what the user can do, *virtual domains* control the devices on which a user can perform those tasks. Virtual domains are described in Create Virtual Domains to Control User Access to Devices, on page 815.

Cisco EPN Manager provides several predefined user groups. If a user belongs to a user group, the user inherits all of the authorization settings for that group. A user is normally added to user groups when their account is created.

These topics explain how to manage user authorization:

- Types of User Groups, on page 793

- View and Change the Tasks a User Can Perform, on page 794
- View and Change the Groups a User Belongs To, on page 795
- View User Groups and Their Members, on page 795
- Create a Customized User Group, on page 806
- View and Change the Tasks a Group Can Perform, on page 807
- Use Cisco EPN Manager User Groups with RADIUS and TACACS+, on page 807

Types of User Groups

Cisco EPN Manager provides the following predefined user groups:

- User Groups—Web UI, on page 793
- User Groups—NBI, on page 794

For information about CLI users, see User Interfaces and User Types, on page 789.

User Groups—Web UI

Cisco EPN Manager provides the default web GUI user groups that are listed in the following table. You can assign users to multiple groups, except for the users that belong to the Monitor Lite user group (because Monitor Lite is for users with limited permissions).

See View and Change the Tasks a Group Can Perform, on page 807 for information on the tasks that pertain to each user group and the default settings.

User Group	Group Task Focus
Root	All operations. The group permissions are not editable. The root web UI user is available after installation and is described in User Interfaces and User Types, on page 789. The best practice is to create other users with Admin or Super Users privileges, and disable the root web UI user as described in Disable and Enable the Web GUI root User, on page 792.
Super Users	All operations (not by default). The group permissions are editable. Can enable permissions similar to those of a root user.
Admin	Administer the system and server. Can also perform monitoring and configuration operations. The group permissions are editable.
Config Managers	Configure and monitor the network (no administration tasks). The permissions assigned to this group are editable.
System Monitoring	Monitor the network (no configuration tasks). The group permissions are editable.
Help Desk Admin	Only has access to the help desk and user preferences-related pages. This is a special group which lacks access to the user interface.
Lobby Ambassador	User administration for Guest users only. Members of this user group cannot be members of any other user group.

User Group	Group Task Focus
User–Defined 1–50	N/A; these are blank groups and can be edited and customized as required.
Monitor Lite	View network topology and use tags. The group permissions are not editable. Members of this user group cannot be members of any other user group.
North Bound API	Access to the SOAP APIs.
User Assistant	Local Net user administration only. Members of this user group cannot be members of any other user group.
mDNS Policy Admin	mDNS policy administration functions.

User Groups—NBI

Cisco EPN Manager provides the default NBI user groups that are listed in the following table. The permissions in these groups are not editable.

See View and Change the Tasks a Group Can Perform, on page 807 for information on the tasks that pertain to each user group and the default settings.

User Group	Provides access to:
NBI Read	RESTCONF NBI read operations (HTTP GET). Can also belong to other NBI and web UI user groups.
NBI Write	RESTCONF NBI write operations (HTTP PUT, POST, DELETE). Can also belong to other NBI and web UI user groups.

View and Change the Tasks a User Can Perform

The tasks a user can perform is controlled by the user groups the user belongs to. Follow these steps to find out the user group and tasks you are authorized to perform.

Note If you want to check the *devices* a user can access, see Assign Virtual Domains to Users, on page 820.

Step 1 Choose **Administration** > **Users** > **Users and Roles**.

Step 2 Choose the **Roles** tab, and locate the user group from the left pane under Roles.

Step 3 Select the user group and choose **Task Permissions** tab, which lists the tasks that group members can and cannot perform.

- Selected check box means the group members can perform that task. If a checked box is greyed-out, it means you cannot disable the task. For example, Cisco EPN Manager does not allow you to remove the "View tags" task for the Monitor Lite user group because it is an integral task for that user group.
- A blank check box means that group members cannot perform that task. If a blank check box is greyed out, it means you cannot enable the task for the user group.

The web GUI root and Monitor Lite groups, and the NBI groups, are not editable.

Step 4 If you want to change permissions, you have these choices:

Note Be careful. Selecting and deselecting tasks in the Group Detail window applies your changes to *all group members*.

- Change permissions for all user group members. See View and Change the Tasks a Group Can Perform, on page 807.
- Add the user to a different user group. The predefined user groups are described in User Groups—Web UI, on page 793 and User Groups—NBI, on page 794. Those topics also describe any group restrictions; for example, if a user belongs to the predefined Monitor Lite user group, the user cannot belong to any other groups.
- Remove the user from this group. See View and Change the Groups a User Belongs To, on page 795.
- Use a customized user group and add the user to that group. To find out which customized groups already exist, see View and Change the Tasks a Group Can Perform, on page 807. To create a new customized group, see Create a Customized User Group, on page 806.

View and Change the Groups a User Belongs To

The tasks users can perform is determined by the user groups they belong to. This is normally configured when a user account is created (see Add and Delete Users, on page 809). User groups are described in Types of User Groups, on page 793.

This procedure explains how to view the groups a user belongs to and, if necessary, change the user's group membership.

Step 1 Choose > **Administration > Users and Roles**, then choose **Users**.

Step 2 In the **User Name** column, locate and select the user name check box. Click the **Edit** option. **Edit User** window appears.

- A checked check box means the user belongs to that group. If a checked box is grayed-out, it means you cannot remove the user from that group. For example, Cisco EPN Manager will not allow you to remove the user named **root** from the root user group.

Step 3 To change the groups the user belongs to, select and unselect the appropriate groups in the **Role Details** drop-down list, then click **Save**.

View User Groups and Their Members

Users can belong to multiple groups, unless they belong to a restricted group such as Monitoring Lite. This procedure explains how to view existing user groups and their members.

Step 1 Choose **Administration** > **Users** > **Users and Roles**, then choose **Roles**.

The Roles page lists all existing user groups and a short list of their members. For a description of these groups, see Types of User Groups, on page 793.

Step 2 To view all members of a group, select a group name and choose **Members** tab.

Step 3 If you want to make changes to these groups, see:

- View and Change the Tasks a Group Can Perform, on page 807
- View and Change the Groups a User Belongs To, on page 795

User Group Permissions and Task Description

The following table describes user group permissions and task descriptions.

Table 57: User Group Permissions and Task Description

Task Group Name	Task Name	Description
Administrative Operations	Device Console Config	Allows user to run configuration commands on Device Console
	Device Console Show	Allows user to run show commands on Device Console
	Export Audit Logs Access	Allows user to access Import Policy Update through Admin Mega menu
	Health Monitor Details	Allows user to modify Site Health Score definitions
	High Availability Configuration	Allows user to configure High Availability for pairing primary and secondary servers
	Import Policy Update	Allow user to manually download and import the policy updates into the compliance and Audit manager engine
	License Center/Smart License	Allows user to access license center/smart license
	Logging	Gives access to the menu item which allows user to configure the logging levels
	Scheduled Tasks and Data Collection	Controls access to the screen to view the background tasks
	System Settings	Controls access to the **Administration > System Settings** menu
	User Defined Fields	Allows user to create user defined fields
	User Preferences	Controls access to the **Administration > User Preference** menu.
	View Audit Logs Access	Allows user to view Network and System audits

Task Group Name	Task Name	Description
Alerts and Events	Ack and Unack Alerts	Allows user to acknowledge or unacknowledge existing alarms
	Alarm Policies	Allows user to access alarm policies.
	Alarm Policies Edit Access	Allows user to edit alarm policies
	Delete and Clear Alerts	Allows user to clear and delete active alarms
	Email Notification	Allows user to configure email notification forwarding
	Notification Policies Read Access	Allows user to view alarm notification policy
	Notification Policies Read-Write Access	Allows user to configure alarm notification policy
	Pick and Unpick Alerts	Allows user to pick and unpick alerts
	Troubleshoot	Allows user to do basic troubleshooting, such as traceroute and ping, on alarms
	View Alert Condition	Allows user to view alert condition.
	View Alerts and Events	Allows user to view a list of events and alarms
License Check	License Check	Allows user to check validity of license, Controller license and MSE license
Configure Menu Task	Configure Menu Access	Allows user to access all features under Configuration Menu
	Unsanitized Device Config Export	Allows user to expose unsanitized Configuration Archive
Diagnostic Tasks	Diagnostic Information	Controls access to diagnostic page.
	Unsanitized Device Config Export	Allows user to expose unsanitized Configuration Archive
Feedback and Support Tasks	Automated Feedback	Allows access to automatic feedback
	TAC Case Management Tool	Allows user to open a TAC case

Task Group Name	Task Name	Description
Global Variable Configuration	Global Variable Access	Allows user to access global variables.
Groups Management	Add Group Members	Allows user to add an entity, such as a device or port, to groups
	Add Groups	Allows user to create groups
	Delete Group Members	Allows user to remove members from groups
	Delete Groups	Allows user to delete groups
	Export Groups	Allows user to export groups
	Import Groups	Allows user to import groups
	Modify Groups	Allows user to edit group attributes such as name, parent, and rules
Help Menu Task	Help Menu Access	Allows user to access Help Menu
Home Menu Task	Home Menu Access	Allows user to access Homepage

Task Group Name	Task Name	Description
Job Management	Approve Job	Allows user to submit a job for approval by another user
	Cancel Job	Allows user to cancel the running jobs
	Delete Job	Allows user to delete jobs from job dashboard
	Edit Job	Allows user to edit jobs from job dashboard
	Pause Job	Allows user to pause running and system jobs
	Schedule Job	Allows user to schedule jobs
	View Job	Allows user to view scheduled jobs.
	Config Deploy Edit Job	Allows user to edit config delployed jobs
	Device Config Backup Job Edit Access	Allows user to change the external backup settings such as repository and file encrytion password
	Job Notification Mail	Allows user to configure notification mails for various job types
	Run Job	Allows user to run paused and scheduled jobs
	System Jobs Tab Access	Allows user to view the system jobs
Monitor Menu Task	Monitor Menu Access	Allows user to access all features under Monitor Menu

Task Group Name	Task Name	Description
Network Configuration	Add Device Access	Allows user to add devices to Cisco EPN Manager
	Admin Templates Write Access	Check thois check-box for enabling admin templates write access for user defind role
	Auto Provisioning	Allows access to auto provisioning
	Alarm Monitor Policies	Allows access to Alarm monitor policies
	Compliance Audit Fix Access	Allows user to view, schedule and export compliance fix job/ report
	Compliance Audit PAS Access	Allows user to view, schedule and export "PSIRT" and "EOX" job/ report
	Compliance Audit Policy Access	Allows user to create, modify, delete, import and export compliance policy
	Compliance Audit Profile Access	Allows user to view, schedule and export compliance audit job or report view and download violations summary
	Compliance Audit Profile Edit Access	Allows user to create, modify and delete compliance profiles view and schedule export compliance audit job or report view and download violations summary
	Config Archive Read Task	Allows config archive read access
	Config Archive Read-Write Task	Allows config archive read-write access
	Configuration Templates Read Access	Allows to access configuration templates in read only mode
	Configure Config Groups	Allows access to Config Group
	Configure ISE Servers	Allows users to manage ISE servers on Cisco EPN Manager
	Configure Templates	Allow the user to do the CRUD operation of Feature Templates and configuration Template
	Credential Profile Add_Edit Access	

Task Group Name	Task Name	Description
		Allows user to Add and edit credential profile
	Credential Profile Delete Access	Allows user to delete credential profile
	Credential Profile View Access	Allows user to view credential profile
	Delete Device Access	Allows user to delete devices from Cisco EPN Manager
	Deploy Configuring Access	Allows user to deploy Configuration and IWAN templates
	Design Configuration Template Access	Allows user to create Configuration > Shared Policy Object templates and Configuration Group templates
	Device Bulk Import Access	Allows user to perform bulk import of devices from CSV files
	Device View configuration Access	Allows user to configure devices in the Device Work Center
	Edit Device Access	Allows user to edit device credentials and other device details
	Export Device Access	Allows user to export the list of devices, including credentials, as a CSV file.
	Network Devices	Allows user to access to the Network devices
	Network Topology Edit	Allows user to create devices, links and network in the topology map, edit the manually created link to assign the interface
	Provisioning Access	Allows access to Provisioning
	QoS Profile Configuration Access	Allows user to create, modify, delete QoS profil;es and schedule QoS profiles deployment job or associate/disassociate interface and Import/Export QoS discovered profiles

Task Group Name	Task Name	Description
Network Monitoring	Admin Dashboard Access	Allows user to access the Admin Dashboard
	Chassis View Read	Allows chassis view read access
	Chassis View Read-Write	Allows chassis view read-write access
	Config Audit Dashboard	Allows users to access Config Audit Dashboard
	Data Collection Management Access	Allow user to access the Assurance Data Sources page
	Details Dashboard Access	Allow user to access the Detail dashboards
	Incidents Alarms Events Access	Allows user to access incidents alarms events.
	Latest Config Audit Report	Allows user to view the latest config audit reports
	Network Topology	Allows users to launch the Network Topology map and view the devices and links in the map
	Performance Dashboard Access	Allow user to access the Performance dashboard
OTDR	OTDR Configure Profiles	Allows access to OTDR configure profiles
	OTDR run scans	Allows user access to OTDR scans
	OTDR Set Baselines	Allows access to OTDR baselines.
	OTDR View Scan results	Allows user to view OTDR scan results
Product Usage	Product Feedback	Allows user to access Help Us Improve page

Task Group Name	Task Name	Description
Reports	Device Reports	Allow user to run reports specific to monitoring specific report related to Devices
	Device Reports Read Only	Allows user to read generated device reports
	Network Summary Reports	Allows user to create and run network summary reports
	Network Summary Reports Read Only	Allows user to view all Summary reports
	Optical Performance Reports	Allows user to create Optical performance reports
	Optical Performance Reports Read Only	Allows user to view Optical performance reports
	Performance Reports	Allows user to create performance reports
	Performance Reports Read Only	Allows user to view performance reports
	Report Launch Pad	Allows user to access the Report page
	Report Run History	Allows user to view report history
	Run Reports List	Allows user to run reports
	Saved Reports List	Allows user to save reports
	System Monitoring Reports	Allows user to view System Monitoring Reports
	Virtual Domains List	Allows user to create the Virtual Domain related report

Task Group Name	Task Name	Description
Software Image Management	Add Software Image Management Servers	Allows user to add software imagemanagement servers
	Image Details View	Allows user to view the image details
	Manage Protocol	Allows user to manage the Protocols
	Swim Access Privilege	Swim Access Privilege
	Swim Activation	Swim Activation
	Swim Collection	Swim Collection
	Swim Delete	Swim Delete
	Swim Distribution	Swim Distribution
	Swim Preference Save	Allows user to save preference options on System Settings à Image Management page
	Software Info Update	Allows the user to edit and save image properties such as minimum RAM, minimum FLASH and minimum boot ROM version
	Swim Recommendation	Allows user to recommend images from Cisco.com and from the local repository
	Swim Upgrade Analysis	Allows user to analyze software images to determine if the hardware upgrades (boot ROM, flash memory, RAM, and boot flash, if applicable) are required before performing a software upgrade

Task Group Name	Task Name	Description
User Administration	Audit Trails	Allows user to access the Audit trails on user login and logout
	LDAP Server	Allows user to access the LDAP Server menu
	RADIUS Servers	Allows user to access the RADIUS Servers menu
	SSO Server AAA Mode	Allows user to access the AAA menu
	SSO Servers	Allows user to access the SSO menu
	TACACS+ Servers	Allows user to access the TACACS+ Servers menu
	Users and Groups	Allows user to access the Users and Groups menu
	Virtual Domain Management	Allows user to access the Virtual Domain Management menu
	Virtual Elements Tab Access	When creating virtual domain or adding members to a virtual domain, allows uses to access the virtual elements tab, so as to allow user to add virtual elements (Datacenters, Clusters and Hosts) to virtual domain
View Online Help	OnlineHelp	Allows user to access the online help

Create a Customized User Group

Cisco EPN Manager provides a set of predefined user groups that help you control user authorization. These groups are described in Types of User Groups, on page 793 and include four User Defined groups which you can customize to create a user group that is specific to your deployment. The following procedure explains how to create a customized group using one of the four predefined User Defined group templates.

Step 1 Choose **Administration** > **Users** > **Users and Roles** , then choose **Roles**.

Step 2 Locate and select a User Defined group that has no members in the left-side Roles pane.

Step 3 Customize the group permissions by checking and unchecking tasks in the **Role Permissions** window. If a task is greyed-out, it means you cannot adjust its setting. You can rename any of the user groups by clicking the **Edit** icon in front of the User Defined group name.

Step 4 Click **Save** to save your group settings.

Step 5 Add members to your group by editing the relevant user accounts and adding the user to your new group. See Add and Delete Users, on page 809 for information on adjusting user accounts.

View and Change the Tasks a Group Can Perform

Follow these steps to get information about existing user groups and the tasks group members can perform. The predefined user groups are described in View User Groups and Their Members, on page 795.

Note If you want to change *device* access, see Assign Virtual Domains to Users, on page 820.

Step 1 Choose **Administration** > **Users** > **Users and Roles**, then choose **Roles**.

The Roles page lists all existing user groups.

Step 2 Select a user group. The **Role Permissions** window lists the tasks permissions.

- A checked task means that group members have permission to perform that task. If a checked box is grayed-out, you cannot disable the task.
- A blank check box means that group members cannot perform that task. If a blank check box is grayed out, you cannot enable the task for the user group.

The web GUI root and Monitor Lite groups, and the NBI groups, are not editable.

Step 3 If you want to change the group permissions—which affects *all group members*—check and uncheck tasks, then click **Save**.

Note Be careful. Selecting and deselecting tasks in the Group Detail window applies your changes to *all group members*. An alternative is to create a new group using one of the User Defined group templates; see Create a Customized User Group, on page 806.

Use Cisco EPN Manager User Groups with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the user groups that exist in Cisco EPN Manager. You can do this using the procedure in Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+, on page 807.

Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all Cisco EPN Manager user group and role information into your Cisco Access Control Server (ACS) or Cisco Identity Services Engine (ISE) server. You can do this using the Task List dialog box provided in the Cisco EPN Manager web GUI. If you do not export the data into your Cisco ACS or Cisco ISE server, Cisco EPN Manager will not allow users to perform their assigned tasks.

The following information must be exported:

- TACACS+—Requires virtual domain and role information (tasks are automatically added).
- RADIUS—Requires virtual domain and role information (tasks are automatically added).

Information in the Task List dialog is preformatted for use with the Cisco ACS server.

Note When you add tasks to the external server, be sure to add the **Home Menu Access** task. It is mandatory for all users.

Step 1 In Cisco Evolved Programmable Network Manager:

a) Choose **Administration** > **Users** > **Users and Roles** > **Roles**.
b) From the Roles list, select the user group, and copy the role for each user group by clicking the **Task List** icon (in front of Role Permissions).
   - If you are using RADIUS, right-click the *role0 line* in the RADIUS Custom Attributes field and choose **Copy**.
   - If you are using TACACS+, right-click the *role0 line* in the TACACS+ Custom Attributes field, and choose **Copy**.

Step 2 Paste the information into your Cisco ACS or Cisco ISE server. These steps show how to add the information to an existing user group in Cisco ACS. If you have not yet added this information to Cisco ACS or Cisco ISE, see:

- Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 831
- Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 825

a) Navigate to **User or Group Setup**.
b) For the applicable user or group, click **Edit Settings**.
c) Paste the attributes list into the appropriate text box.
d) Select the check boxes to enable these attributes, then click **Submit + Restart**.

Add Users and Manage User Accounts

Create Web GUI Users with Administrator Privileges

After installation, Cisco EPN Manager has a web GUI root account named **root**. This account is used for first-time login to the server to create:

- Web GUI users with Administrator privileges who manage the product and features.
- All other user accounts.

You should *not* use the web GUI root account for normal operations. For security purposes, create a new web GUI user with Administrator privileges (and access to all devices), and then disable the web GUI root account.

Step 1 Choose **Administration** > **Users** > **Users and Roles**, then choose **Users**.

Step 2 On the **Users** window, click + to display a new user entry in the table.

Step 3 Enter the username in the **User Name** text box.

Step 4 Enter a password. The new password must satisfy the conditions specified in the password policy. Click the **?** icon to view the password policy.

Step 5 (Optional) Enter the **First Name**, **Last Name**, and **Description** for the user.

Step 6 Enter the email address in the **Email Address** text box.

Step 7 In the **Role** drop-down list, choose **Admin**.

Step 8 From the **Virtual Domains**, specify which devices the user can access. You should have at least one Admin web GUI user that has access to all devices (ROOT-DOMAIN). For more information on virtual domains, see Create Virtual Domains to Control User Access to Devices, on page 815.

Note If you select a parent virtual domain the child (subordinate) virtual domains under it will also get selected.

Step 9 Click **Save**.

Note When you create a new user, do not autofill or save the user credentials in the browser.

What to do next

For security purposes, disable the web GUI root account as described in Disable and Enable the Web GUI root User, on page 792.

Add and Delete Users

Before you create user accounts, create virtual domains to control device access so you can apply them during account creation. Otherwise you must edit the user account to add the domain access. See Create Virtual Domains to Control User Access to Devices, on page 815.

If you want to temporarily disable an account (rather than delete it), see Disable (Lock) a User Account, on page 810.

Step 1 Choose **Administration** > **Users** > **Users and Roles**, then choose **Users**.

Step 2 Click + to display a new user entry.

Step 3 Configure the user account.

a) Enter a username and password.

Note To autogenerate the password, enter the username and the email address. For more information, see Auto-generate a User's Password, on page 811.

b) Enter the first name, last name, and a description for the user.
c) Control the actions that the user can perform by selecting one or more user groups. For descriptions of user groups, see View User Groups and Their Members, on page 795.
d) Control the devices that a user can access from the **Virtual Domains** space and assigning domains to the user. (See Create Virtual Domains to Control User Access to Devices, on page 815.)

Step 4 Click **Save**.

Note When you create a new user, do not autofill or save the user credentials in the browser.

Step 5 To delete user accounts, select a user, and click .

Step 6 Click **Delete** to confirm that you want to delete the user.

Disable (Lock) a User Account

Disable a user account when you temporarily want to disallow a user from logging in to the Cisco EPN Manager GUI. You might want to do this if a user is temporarily changing job functions. If the user tries to log in, Cisco EPN Manager displays a message saying the login failed because the account is locked. You can unlock the account later without having to re-create the user. If you want to delete a user account, see Add and Delete Users, on page 809.

User accounts may be disabled automatically if the password is not changed before expiration. Only an administrator can reset the password in this case. See Change a User's Password, on page 810 and Configure Global Password Policies for Local Authentication, on page 813.

Step 1 Choose **Administration** > **Users** > **Users and Roles**, then click **Users**.

Step 2 Select the user whose access you want to disable or enable.

Step 3 Click to lock the user (or **Unlock User(s)** to unlock the user).

Change a User's Password

You can configure password rules to force users to change their passwords (see Configure Global Password Policies for Local Authentication, on page 813). Users can change their own passwords as described in Change Your Password, on page 3. To change a user's password manually, use this procedure:

Step 1 Choose **Administration** > **Users** > **Users and Roles**, then click **Users**.

Step 2 Select the username and click icon, which opens the Edit User window.

Step 3 Enter the new password in the password fields and click **Save**.

Auto-generate a User's Password

Cisco EPN Manager offers you the option to auto-generate the password for new and existing users based on the email server availability. If this option is enabled, the system sends an email to the user with password details.

Note The **Auto-generate Passwords** option is available only if the email server is configured.

To auto-generate the password and email it to the user, follow this procedure:

Before you begin

Configure the email sever. For more information, see Set Up the SMTP E-Mail Server, on page 767.

Step 1 Choose **Administration** > **Users** > **AAA**, select **Settings**, and expand the **Local Password Policy** drop-down.

Step 2 Select the **Auto-generate Passwords** check box.

Step 3 Click **Save All Changes** to save your changes.

Step 4 Go to **Administration** > **Users** > **Users and Roles**, then click **Users**.

a) For a new user, enter the user name and email address.

b) For an existing user, reset the password.

Step 5 Click **Save** to save your changes and send an email notification to the user.

Find Out Which Users Are Currently Logged In

Use this procedure to find out who is currently logged into the Cisco EPN Manager server. You can also view a historical list of the actions performed by the user in the current web GUI session and past sessions.

Note By default, Cisco EPN Manager displays 50 records without pagination for the subsequent records. To view more than 50 records, click the settings icon at the top-right corner of the screen and enter the required value in **My Preferences** > **General** > **Items per Page List** field.

Step 1 Choose **Administration** > **Users** > **Users and Roles**, then choose **Active Sessions** tab. Cisco EPN Manager lists all users that are currently logged in to the Cisco EPN Manager server, including their client machine IP address.

Step 2 To view a historical list of all actions performed by this user, click the icon that corresponds to the user name, and choose **Audit Trail**. If the user performed any actions on managed devices (for example, the user added new devices to Cisco EPN Manager), the device IP addresses are listed in the Device IP Address column.

Step 3 If you want to end an active user session, click , and choose **Terminate Session**.

Note **Terminate Session** terminates only an active user session. If you want to prevent the user from logging back in again, see Disable (Lock) a User Account, on page 810.

View the Tasks Performed By Users (Audit Trail)

Cisco EPN Manager maintains a history of all actions performed by users in active and past web GUI sessions. Follow these steps to view a historical list of tasks performed by a specific *user* or by all members of a specific *user group*. The audit information includes a description of the task, IP address of the client from which the user performed the task, and the time at which the task was performed. If a task affects a managed device (for example, a user adds a new device or issues commands on a network element through the **Device Console**), the affected device's IP address is listed in the Device IP Address column. If a change is made to multiple devices (for example, a user deploys a configuration template to 10 switches), Cisco EPN Manager displays an audit entry for each switch.

To find out which users are currently logged into the Cisco EPN Manager web GUI, see Find Out Which Users Are Currently Logged In, on page 811.

To view audits that are not user-specific, see these topics:

- Audit Changes Made By Users (Change Audit), on page 863

Step 1 Choose **Administration** > **Users** > **Users and Roles**.

Step 2 To view the tasks performed by a specific user:

a. Choose **Users**.

b. Locate the user name, click the  icon, and choose **Audit Log**.

Step 3 To view a historical list of the tasks performed by all members of a user group:

a. Choose **Roles**.

b. Locate the user group name and click the **Members** tab. Click the  icon corresponding to that group and choose **Audit Trail**.

Configure Job Approvers and Approve Jobs

Use job approval when you want to control jobs that could significantly impact the network. If a job requires approval, Cisco EPN Manager sends an e-mail to all users with Admin privileges, and does not run the job until one of them approves it. If a job is rejected by an approver, the job is removed from the database. By default, all jobs do not require approval.

If job approval is already enabled and you want to view jobs that need approval, approve a job, or reject a job, choose **Administration** > **Dashboards** > **Job Dashboard**, and click the **Job Approval** link at the top-right corner of the window.

- For a rollback job, it displays the running configuration and start-up configuration details.
- For an overwrite job, it explains the operation to be performed.

To enable job approval and configure the jobs that require approval before running:

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Job Approval**.

Step 2 Check the **Enable Job Approval** checkbox. Enabling this checkbox lets you choose from Job Type Order list. Choose the required option.

Step 3 Check the **Enable Mail for Job Approval** checkbox. By default this checkbox is unchecked. Enter the email addresses of the job approvers.

Step 4 Click **Save**.

Configure Global Password Policies for Local Authentication

If you are using local authentication (Cisco EPN Manager authentication mechanism), you control the global password policies from the web GUI. If you are authenticating Cisco EPN Manager users using external authentication, the policies are controlled by an external application (see Set Up External Authentication Using the CLI, on page 720).

By default, users are not forced to change passwords after any period of time. To enforce password changes and configure other password rules, choose **Administration** > **Users** > **AAA**, choose **Settings**, and expand the **Local Password Policy** drop-down.

Note You must select the **Change password** on the first login check box to prompt the new users to change the default password on their initial login to Cisco EPN Manager. Deselecting this checkbox launches the Home Dashboard page on logging in.

Configure Number of Parallel Sessions Allowed

Note This setting applies only to the sessions logged in from the Cisco EPN Manager web-interface.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

Step 2 Under **Parallel Sessions**, enter a value between 1 and 15 in the **Number of parallel sessions allowed** field.

Step 3 Click **Save**. You need to restart the system for this change to take effect.

Configure the Global Timeout for Idle Users

Cisco EPN Manager provides settings that control when and how idle users are automatically logged out:

- User Idle Timeout—You can disable or configure this setting, which ends your user session automatically when you exceed the timeout. It is enabled by default and is set to 10 minutes.
- Global Idle Timeout—The Global Idle Timeout setting overrides the User Idle Timeout setting. The Global Idle Timeout is enabled by default and is set to 10 minutes. Only users with administrative privileges can disable the Global Idle Timeout setting or change its time limit.

The Idle Timeout feature starts functioning when the browser is open, but there is no user interaction. It means that, if the idle timeout is 10 minutes and the browser is open and user does not have any key strokes or mouse clicks, then the user will be logged out after 10 minutes of inactivity. However, if the browser is killed without logging out from Cisco EPN Manager, by default, the session expires in 60 minutes regardless of the idle timeout value set in Cisco EPN Manager.

By default, client sessions are disabled and users are automatically logged out after 15 minutes of inactivity. This is a global setting that applies to all users. For security purposes, you should not disable this mechanism, but you can adjust the timeout value using the following procedure. To disable/change the timeout for an idle user, see Disable Idle User Timeout, on page 814.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

Step 2 In the **Global Idle Timeout** area, make sure the **Logout all idle users** check box is selected (this means the mechanism is enabled).

Step 3 Configure the timeout by choosing a value from the **Logout all idle users after** drop-down list.

Step 4 Click **Save**. You will must log out and log back in for this change to take effect.

Disable Idle User Timeout

By default, client sessions are disabled and users are automatically logged out after certain period of inactivity. This is a global setting that applies to all users. To avoid being logged out during the installation, it is recommended to disable automatic logout of idle users in the system settings using the following procedure.

Note The Global Idle Timeout setting overrides the User Idle Timeout setting. To configure Global Idle Timeout settings, see Configure the Global Timeout for Idle Users, on page 814.

Irrespective of the customer disabling the "Logout all idle users" in system settings and / Or disabling the "Logout idle user" in the Root user my preference setting, the session will ultimately be timed out once the web-server's session time-out is reached. This is essentially to maintain the security posture. For more guidelines on increasing/decreasing the session time-out, see https://owasp.org/www-community/Session_Timeout

Note Session will be timed out only if it is inactive whereas active user sessions are not timed.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.

Step 2 In the **Global Idle Timeout** area, uncheck the **Logout all idle users** check box and click **Save**.

Step 3 Click ⚙ at the top right of web GUI window and choose **My Preferences**.

Step 4 In the **User Idle Timeout** area, uncheck the **Logout idle user** check box and click **Save**.

If you must change the idle timeout value, then select **Logout idle user** check box and from the **Logout idle user after** drop-down list, choose one of the idle timeout limits. (But this cannot exceed the value set in the Global Idle Timeout settings.)

Step 5 Click **Save**. You must log out and log back in for this change to take effect.

Create Virtual Domains to Control User Access to Devices

What Are Virtual Domains?

Virtual domains are logical groupings of devices, sites, and other NEs, and are used to control who has access to those NEs. You choose which elements are included in a virtual domain and which users have access to that virtual domain. Virtual domains can be based on physical sites, device types, user communities, or any other designation you choose. All devices belong to ROOT-DOMAIN, which is the parent domain for all new virtual domains.

Virtual domains work in conjunction with user groups. Virtual domains control the devices a user can access, while user groups determine the actions a user can perform on those devices. Users with access to a virtual domain (depending on their privileges) can configure devices, view alarms, and generate reports for the NEs in their virtual domain.

You can create virtual domains after you have added devices to Cisco EPN Manager. Each virtual domain must have a name and can have an optional description, email address, and time zone. Cisco EPN Manager uses the email address and time zone that you specify to schedule and email domain-specific reports.

Users work in one virtual domain at a time. Users can change the current virtual domain by choosing a different one from the Virtual Domain drop-down list (see Work In a Different Virtual Domain , on page 23).

Before you set up virtual domains, determine which users are responsible for managing particular areas of the network. Then organize your virtual domains according to those needs—for example, by geography, by device type, or by the user community served by the network.

How Virtual Domains Affect Cisco EPN Manager Features

Virtual domains are organized hierarchically. The ROOT-DOMAIN domain includes all virtual domains.

Because network elements are managed hierarchically, user views of devices—as well as some associated features and components—are affected by the user's virtual domain. The following topics describe the effects of virtual domains on these features.

Reports and Virtual Domains

Reports only include components that belong to the active virtual domain. A parent virtual domain cannot view reports from its child domains. New components are only reflected in reports that are generated after the components were added.

Search and Virtual Domains

Search results only include components that belong to the active domain. You can only view saved search results if you are in the same domain from which the search was performed and saved. When working in a parent domain, you cannot view the results of searches performed in child domains.

Alarms and Virtual Domains

When a component is added to a virtual domain, no previous alarms for that component are visible to that virtual domain . Only new alarms are visible. For example, if a network element is added to Cisco EPN Manager, and that network element generated alarms before and after it was added, its alarm history would only include alarms generated after it was added.

Note For alarm email notifications, only the ROOT-DOMAIN virtual domain can enable Location Notifications, Location Servers, and Cisco EPN Manager email notifications.

Maps and Virtual Domains

Maps only display network elements that are members of the active virtual domain.

Configuration Templates and Virtual Domains

When you create or discover a configuration template in a virtual domain, it can only be applied to network elements in that virtual domain. If you apply a template to a device and then add that device to a child domain, the template is also available to the same device in the child domain.

Note If you create a child domain and then apply a configuration template to both network elements in the virtual domain, Cisco EPN Manager might incorrectly reflect the number of partitions to which the template was applied.

Config Groups and Virtual Domains

A parent domain can view the network elements in a child domain's configuration groups. The parent domain can also edit the child domain's configuration groups.

Email Notifications and Virtual Domains

Email notifications can be configured per virtual domain.

For *alarm* email notifications, only the ROOT-DOMAIN can enable Location Notifications, Location Servers, and email notifications.

Create New Virtual Domains

To create a new virtual domain, use one of the following procedures depending on the desired hierarchy of the virtual domain.

To create a new virtual domain (*new-domain*) here:	**See this procedure:**
ROOT-DOMAIN > ***new-domain***	Create Virtual Domains Directly Under ROOT-DOMAIN, on page 818
ROOT-DOMAIN > *existing-domain* > ***new-domain***	Create Child Virtual Domains (Sub-domains), on page 818
ROOT-DOMAIN > *existing-domain* > *existing-domain* > ***new-domain***	
(etc.)	

Create Virtual Domains Directly Under ROOT-DOMAIN

The following procedure creates an empty virtual domain under ROOT-DOMAIN. You can also create multiple virtual domains at one time by using the procedure in Import a List of Virtual Domains, on page 818.

If a virtual domain exists under ROOT-DOMAIN, and you want to create a new domain under it (a child domain), see Create Child Virtual Domains (Sub-domains), on page 818.

Step 1 Choose **Administration** > **Users** > **Virtual Domains**.

Step 2 In the Virtual Domains sidebar menu, click the ***i*** (info) icon and click **Create Sub Domain**.

Step 3 Enter the name and description for the domain.

Step 4 Click **Submit** to view a summary of the newly created virtual domain.

What to do next

Add devices to the virtual domain as described in Add Network Devices to Virtual Domains, on page 819.

Create Child Virtual Domains (Sub-domains)

The following procedure creates a child virtual domain (also called a subdomain). A child virtual domain is a domain that is *not* directly under ROOT-DOMAIN; it is under a domain that is under ROOT-DOMAIN.

Do not use this procedure if you want the new virtual domain to appear directly under ROOT- DOMAIN. In that case, see Create Virtual Domains Directly Under ROOT-DOMAIN, on page 818.

Step 1 Choose **Administration** > **Users** > **Virtual Domains**.

Step 2 In the Virtual Domains sidebar menu:

a) Locate the domain under which you want to create a new child domain. (This is called the parent domain.)

b) Click the information (**i**) icon next to the domain name. This opens a data popup window.

c) In the popup window, click **Add a Sub Domain**. The navigation pane switches to the list view, with the parent domain displayed above the child domain named **Untitled**.

Step 3 Enter a name in the **Name** text box. The name in the navigation pane will change from **Untitled** to the **child domain name** after you save the new child domain.

Step 4 (Optional) Add a description.

Step 5 Click **Create** and confirm the creation of the new child domain.

What to do next

Add devices to the virtual domain as described in Add Network Devices to Virtual Domains, on page 819.

Import a List of Virtual Domains

If you plan to create many virtual domains, or give them a complex hierarchy, you will find it easier to specify them in a properly formatted CSV file, and then import it. The CSV format allows you to specify a name,

description, time zone, and email address for each virtual domain you create, as well as each domain's parent domain. Adding network elements to the virtual domains must be performed separately.

Step 1 Choose **Administration** > **Users** > **Virtual Domains**.

Step 2 Click the **Import Domain(s)** icon, download a sample CSV file from the link provided in the popup, and prepare the CSV file.

Step 3 Click **Choose File** and navigate to your CSV file.

Step 4 Click **Import** to import the CSV and create the virtual domains you specified.

What to do next

Add devices to the virtual domains as explained in Add Network Devices to Virtual Domains, on page 819.

Add Network Devices to Virtual Domains

Use this procedure to add network devices to a virtual domain. When you add a new network device to an existing virtual domain, the device becomes immediately accessible to users with access to that domain (users do not have to restart the web GUI).

Step 1 Choose **Administration** > **Users** > **Virtual Domains**.

Step 2 From the Virtual Domains sidebar menu, click the virtual domain to which you want to add network devices.

Step 3 Click the **Add** icon from the left-pane.

Step 4 You can either add network devices by group or add a network device to a specific location group.

Step 5 To add devices from groups, select the **Groups** tab, click **Add**, and the **Add Group** pop-up appears, which lists the applicable location and user-defined groups. Select the group to add the device and click **Select** to add the groups to the Selected Network Devices by Group table.

Step 6 To add individual devices, select the **Network Devices** tab, click **Add** and the **Select Network Devices** pop-up appears. Here, a **Filter By** drop-down list is available to filter the network devices based on functionality.

Step 7 From the **Filter By** drop-down list, choose a network device. Select the required devices from the Available Network Devices table and click **Select** to add the devices to the Selected Network Devices table.

Note Select Network Devices dialog lists all managed devices, not only those that are in the parent domain. If you add a device that is not included in the parent domain, Cisco EPN Manager adds it to the child and parent domain.

Note You cannot add more than 500 network devices in a single shot using **Select All** function. To add more than 500 devices, use the **Filter By** option multiple times.

Step 8 Click **Submit** to view the summary of the virtual domain contents.

Step 9 Click **Save** to confirm your changes.

What to do next

Give users access to the virtual domain as described in Assign Virtual Domains to Users, on page 820.

Assign Virtual Domains to Users

Once a virtual domain is assigned to a user account, the user is restricted to viewing and performing operations on the devices in their assigned domain(s).

Note When using external AAA, be sure to add the custom attributes for virtual domains to the appropriate user or group configuration on the external AAA server. See Use Cisco EPN Manager Virtual Domains with RADIUS and TACACS+, on page 821.

Step 1 Choose **Administration** > **Users** > **Users and Roles** > **Users**.

Step 2 Select the user to grant device access. Click the icon, which opens the Edit User window.

Step 3 From the **Virtual Domains** space, add or remove domains by checking or unchecking the checkboxes, and click **Save**.

Edit a Virtual Domain

To adjust a virtual domain, choose it from the Virtual Domain Hierarchy on the left sidebar menu to view or edit its assigned network devices. You cannot edit any of the settings for ROOT-DOMAIN.

Step 1 Choose **Administration** > **Users** > **Virtual Domains**.

Step 2 Click the virtual domain you want to edit in the Virtual Domains sidebar menu.

Step 3 To adjust the name, email address, time zone or description, enter your changes in the text boxes.

Step 4 To adjust device members:

- To add devices, click **Add** and follow the instructions in Add Network Devices to Virtual Domains, on page 819.
- To delete devices, select the devices using their check boxes, then click **Delete**.

Step 5 Click **Save** to apply and save your changes.

Delete a Virtual Domain

Use this procedure to delete a virtual domain from Cisco EPN Manager. This procedure only deletes the virtual domain; it does not delete the network elements from Cisco EPN Manager (the network elements will continue to be managed by Cisco EPN Manager).

Before you begin

You can only delete a virtual domain if:

- It is not the only domain a user can access. In other words, if a Cisco EPN Manager user has access to *only* that domain, you cannot delete it.
- No users are logged into the domain.

Step 1 Choose **Administration** > **Users** > **Virtual Domains**.

Step 2 In the Virtual Domains sidebar menu, click the information (**i**) icon next to the virtual domain name. This opens a data popup window.

Step 3 In the popup window, click **Delete**.

Step 4 Click **OK** to confirm deleting the virtual domain.

Use Cisco EPN Manager Virtual Domains with RADIUS and TACACS+

Your RADIUS or TACACS+ servers must be configured to recognize the virtual domains that exist in Cisco EPN Manager. You can do this using the procedure in Export the Cisco Evolved Programmable Network Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 821 .

If your RADIUS or TACACS+ server does not have any virtual domain information for a user, the following occurs, depending on the number of virtual domains that are configured in Cisco EPN Manager:

- If Cisco EPN Manager has only one virtual domain (ROOT-DOMAIN), the user is assigned the ROOT-DOMAIN by default.
- If Cisco EPN Manager has multiple virtual domains, the user is prevented from logging in.

Export the Cisco Evolved Programmable Network Manager Virtual Domain Attributes for RADIUS and TACACS+

If you are using RADIUS or TACACS+, you must copy all Cisco Evolved Programmable Network Manager virtual domain information into your Cisco ACS or Cisco ISE server. You can do this using the Virtual Domains Custom Attributes dialog box provided in the Cisco Evolved Programmable Network Manager web GUI. If you do not export the data into your Cisco ACS or Cisco ISE server, Cisco Evolved Programmable Network Manager will not allow users to log in.

The following information must be exported, depending on the protocol you are using:

- TACACS+—Requires virtual domain, role, and task information.
- RADIUS—Requires virtual domain and role information (tasks are automatically added).

When you create a child domain for an existing virtual domain, the sequence numbers for the RADIUS/TACACS+ custom attributes are also updated in the parent-virtual domain. These sequence numbers are for representation only and do not impact AAA integration.

Information in the Virtual Domains Custom Attributes dialog is preformatted for use with Cisco ACS server.

Note When you add tasks to the external server, be sure to add the **Home Menu Access** task. It is mandatory for all users.

Before you begin

Make sure you have added the AAA server and configured the AAA mode as explained in Configure External Authentication, on page 823.

Step 1 In Cisco Evolved Programmable Network Manager:

a) Choose **Administration** > **Users** > **Virtual Domains**.

b) Click **Export Custom Attributes** at the top right of the window. This opens the Virtual Domain Custom Attributes dialog.

c) Copy the attributes list.

- If you are using RADIUS, right-click *all of the text* in the RADIUS Custom Attributes field and choose **Copy**.
- If you are using TACACS+, right-click *all of the text* in the TACACS+ Custom Attributes field and choose **Copy**.

Step 2 Paste the information into your Cisco ACS or Cisco ISE server. These steps show how to add the information to an existing user group in Cisco ACS. If you have not yet added this information to Cisco ACS or Cisco ISE, see:

- Use Cisco ACS With RADIUS or TACACS+ for External Authentication, on page 831
- Use Cisco ISE With RADIUS or TACACS+ for External Authentication , on page 825

a) Navigate to **User or Group Setup**.

If you want to specify virtual domains on a per-user basis, then you must make sure you add all of the custom attributes (for example, tasks, roles, virtual domains) information to the User custom attribute page.

a) For the applicable user or group, click **Edit Settings**.

b) Paste the attributes list into the appropriate text box.

c) Select the check boxes to enable these attributes, then click **Submit + Restart**.

Configure Local Authentication

Cisco EPN Manager uses local authentication by default, which means that user passwords are stored and verified from the Cisco EPN Manager database.

To check the authentication mode:

SUMMARY STEPS

1. Choose **Administration** > **Users** > **AAA** > **Settings**. The selection is displayed on the **AAA Mode Settings** page. If you are using local authentication, make sure to configure password policies. See Configure Global Password Policies for Local Authentication, on page 813.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Choose **Administration** > **Users** > **AAA** > **Settings**. The selection is displayed on the **AAA Mode Settings** page. If you are using local authentication, make sure to configure password policies. See Configure Global Password Policies for Local Authentication, on page 813.	If you want to use SSO with local authentication, see Use SSO With Local Authentication, on page 823. For information on external authentication, see .

Use SSO With Local Authentication

To use SSO with local authentication, you must add the SSO server and then configure Cisco EPN Manager to use SSO in local mode.

If you have deployed Cisco EPN Manager in a high availability environment where you have a primary and backup server, refer to the instructions in Configure an SSO Server in an HA Environment, on page 887.

Cisco EPN Manager does not support localization on the SSO sign-in page.

The following topics describe how to configure SSO for external authentication, but you can use the same procedures to configure SSO for local authentication. The only difference is that when you configure the SSO mode on the Cisco EPN Manager server, choose **Local** mode (not RADIUS or TACACS+).

-
- Add the SSO Server, on page 837
- Configure SSO Mode on the Cisco EPN Manager Server, on page 837

Configure External Authentication

Users with web GUI root user or Super User privileges can configure the Cisco EPN Manager to communicate with external RADIUS, TACACS+, and SSO servers for external authentication, authorization, and accounting (AAA). If you choose to configure external authentication, the user groups, users, authorization profiles, authentication policies, and policy rules must be created in the external server through which all access requests to Cisco EPN Manager will be routed.

You can use a maximum of three AAA servers. Users are authenticated on the second server only if the first server is not reachable or has network problems.

Note You can use up to three AAA servers together, only if they support the same RADIUS, TACACS+ or LDAP protocol. Using servers having different protocols together is not supported. However, if you want to use multiple AAA servers running different protocols, then you must use Cisco ISE or ACS as a proxy between EPNM and the AAA servers. In this case, you need to set up your authentication logic based on the Cisco ISE or Cisco ACS configurations.

If you want to configure external authentication from the CLI, see Set Up External AAA Via CLI.

See the following topics for more information.

- Use RADIUS or TACACS+ for External Authentication

Use RADIUS or TACACS+ for External Authentication

These topics explain how to configure Cisco EPN Manager to use RADIUS or TACACS+ servers.

Add a RADIUS or TACACS+ Server to Cisco EPN Manager

To add a RADIUS or TACACS+ server to Cisco EPN Manager:

Step 1 Choose **Administration** > **Users** > **AAA**, then choose **Servers**. From this window, you can add, edit settings, and delete a new RADIUS/TACACS+ server.

Step 2 Select the type of server that you want to add.

- For RADIUS, click the **RADIUS** tab. Click the  icon.
- For TACACS+, click the **TACACS+** tab. Click the  icon.

Step 3 Enter the required information—IP address, DNS Name, and so forth. For Cisco EPN Manager to communicate with the external authentication server, the shared secret entered on this page must match the shared secret configured on the RADIUS or TACACS+ server. You can use alphabets, numbers, and special characters except **‘** (single quote) and **“** (double quote) while entering the shared secret key for a third-party TACACS+ or RADIUS server. Enter the Retransmit Timeout and the Retries.

Step 4 Select the authentication type.

- PAP—Password-based authentication protocol requires two entities to share a password in advance and use the password for authentication.
- CHAP—Challenge-Handshake Authentication Protocol requires the client and server to know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

Step 5 Click **Test** to check the connectivity of the AAA server. The connectivity test passes only if the port, authentication type, and shared key that you have entered match the TACACS or RADIUS server.

Step 6 Click **Save**.

Step 7 To edit a RADIUS/TACACS+ server:

a) Click the checkbox next to the RADIUS/TACACS+ server and click  . After making changes, click **Save**.

Step 8 To delete a RADIUS/TACACS+ server:

a) Click the checkbox next to the RADIUS/TACACS+ server and click . The Delete dialog box opens. Click **Delete** to confirm.

Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server

Step 1 Choose **Administration** > **Users** > **AAA**, then choose **Settings**.

Step 2 Select **TACACS+** or **RADIUS**.

Step 3 Select the **Fallback to Local** checkbox 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 when the external RADIUS or TACACS+ server goes down, perform the following steps:

a) Select **Fallback to Local**.

b) Specify the fallback conditions:

- **Only on no server response**—only when the external server is unreachable or has network problems. If you select this option, you can login as an AAA user only.
- **On authentication failure or no server response**—either when the external server is unreachable, or has network problems, or the external AAA server cannot authenticate the user. If you select this option, you can login as a local user and an AAA user.

Step 5 Click **Save All Changes**.

Use Cisco ISE With RADIUS or TACACS+ for External Authentication

Cisco Identity Services Engine (ISE) uses the RADIUS or TACACS+ protocols for authentication, authorization, and accounting (AAA). You can integrate Cisco Evolved Programmable Network Manager with Cisco ISE to authenticate the Cisco Evolved Programmable Network Manager users using the RADIUS or TACACS+ protocols. When you use external authentication, the details such as users, user groups, passwords, authorization profiles, authorization policies, and policy rules that are required for AAA must be stored and verified from the Cisco ISE database.

Note Cisco Evolved Programmable Network Manager natively supports LDAP.

Complete the following tasks to use Cisco ISE with the RADIUS or TACACS+ protocol for external authentication:

Tasks to be completed to use Cisco ISE for external authentication	For information, see:
Make sure you are using a supported version of Cisco ISE	Supported Versions of Cisco ISE in Cisco Evolved Programmable Network Manager, on page 826

Add Cisco Evolved Programmable Network Manager as an AAA client in Cisco ISE	Add Cisco Evolved Programmable Network Manager as a Client in Cisco ISE, on page 827
Create a user group in Cisco ISE	Create a User Group in Cisco ISE, on page 827
Create a user in Cisco ISE and add the user to the user group that is created in Cisco ISE	Create a User and Add the User to a User Group in Cisco ISE, on page 828
(If using RADIUS) Create an authorization profile for network access in Cisco ISE, and add the RADIUS custom attributes with user roles and virtual domains created in Cisco Evolved Programmable Network Manager **Note** For RADIUS, you do not need to add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for RADIUS in Cisco ISE, on page 828
(If using TACACS+) Create an authorization profile for network access in Cisco ISE, and add the TACACS+ custom attributes with user roles and virtual domains created in Cisco Evolved Programmable Network Manager **Note** For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for TACACS+ in Cisco ISE, on page 829
Create an authorization policy in Cisco ISE and associate the policy with the user groups and authorization profile created in Cisco ISE	Configure an Authorization Policy in Cisco ISE, on page 826
Create an authentication policy to define the protocols that Cisco ISE must use to communicate with Cisco Evolved Programmable Network Manager, and the identity sources that it uses for authenticating users to Cisco Evolved Programmable Network Manager	Create an Authentication Policy in Cisco ISE, on page 830
Add Cisco ISE as a RADIUS or TACACS+ server in Cisco Evolved Programmable Network Manager	
Configure the RADIUS or TACACS+ mode on the Cisco Evolved Programmable Network Manager server	Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server, on page 825

Supported Versions of Cisco ISE in Cisco Evolved Programmable Network Manager

Cisco Evolved Programmable Network Manager supports Cisco ISE 1.*x* and 2.*x* releases .

Configure an Authorization Policy in Cisco ISE

An authorization policy consists of a rule or a set of rules that are user-defined and produce a specific set of permissions, which are defined in an authorization profile. Based on the authorization profile, access requests to Cisco EPN Manager are processed.

There are two types of authorization policies that you can configure:

- Standard—Standard policies are intended to be stable and are created to remain in effect for long periods of time, to apply to a larger group of users, devices, or groups that share a common set of privileges.
- Exception—Exception policies are created to meet an immediate or short-term need, such as authorizing a limited number of users, devices, or groups to access network resources. An exception policy lets you create a specific set of customized values for an identity group, condition, or permission that are tailored for one user or a subset of users.

For more information about authorization policies, see the "Manage Authorization Policies and Profiles" chapter in the Cisco Identity Services Engine Administrator Guide.

To create an authorization policy in Cisco ISE:

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Policy** > **Authorization**.

Step 3 In the **Standard** area, click the down arrow on the far right and select either **Insert New Rule Above** or **Insert New Rule Below**.

Step 4 Enter the rule name and choose identity group, condition, attribute, and permission for the authorization policy.

For example, you can define a user group as Cisco EPN Manager-System Monitoring-Group and choose this group from the Identity Groups drop-down list. Similarly, define an authorization profile as Cisco EPN Manager-System Monitoring-authorization profile and choose this profile from the Permissions drop-down list. Now, you have defined a rule where all users belonging to the Cisco EPN Manager System Monitoring identity group receive an appropriate authorization policy with system monitoring custom attributes defined.

Step 5 Click **Done**, and then click **Save**.

Add Cisco Evolved Programmable Network Manager as a Client in Cisco ISE

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Administration** > **Network Resources** > **Network Devices**.

Step 3 In the **Network Devices** page, click **Add**.

Step 4 Enter the device name and IP address of the Cisco Evolved Programmable Network Manager server.

Step 5 Check the **Authentication Settings** check box, and then enter the shared secret.

Note Ensure that this shared secret matches the shared secret you enter when adding the Cisco ISE server as the RADIUS server in Cisco Evolved Programmable Network Manager.

Step 6 Click **Submit**.

Create a User Group in Cisco ISE

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Administration** > **Identity Management** > **Groups**.

Step 3 In the **User Identity Groups** page, click **Add**.

Step 4 In the **Identity Group** page, enter the name and description of the user group.

Step 5 Click **Submit**.

Create a User and Add the User to a User Group in Cisco ISE

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Administration** > **Identity Management** > **Identities**.

Step 3 In the **Network Access Users** page, click **Add**.

Step 4 From the **Select an item** drop-down list, choose a user group to assign the user to.

Step 5 Click **Submit**.

Create an Authorization Profile for RADIUS in Cisco ISE

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the RADIUS custom attributes that are associated with user roles, tasks, and virtual domains created in Cisco Evolved Programmable Network Manager.

Note For RADIUS, you can add the user role attributes without adding the task attributes. The tasks are automatically added with the user roles.

For more information about Cisco ISE authorization profiles, see the information on managing authorization policies and profiles in the Cisco Identity Services Engine Administrator Guide.

To create an authorization profile for RADIUS in Cisco ISE:

Before you begin

Make sure you have the complete list of the following Cisco Evolved Programmable Network Manager custom attributes for RADIUS. You will need to add this information to Cisco ISE in this procedure.

- Cisco Evolved Programmable Network Manager user roles and tasks—see Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+, on page 807
- Cisco EPN Manager virtual domains—see Export the Cisco Evolved Programmable Network Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 821

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Policy** > **Policy Elements** > **Results**.

Step 3 From the left sidebar, choose **Authorization** > **Authorization Profiles**.

Step 4 In the **Standard Authorization Profiles** page, click **Add**.

Step 5 In the **Authorization Profile** page, enter the name and description of the authorization profile.

Step 6 From the **Access Type** drop-down list, choose **ACCESS_ACCEPT**.

Step 7 In the **Advanced Attributes Settings** area, paste in the complete list of RADIUS custom attributes for:

- User roles
- Virtual domains

Note If you do add user tasks, be sure to add the Home Menu Access task. It is mandatory.

Step 8 Click **Submit**.

Create an Authorization Profile for TACACS+ in Cisco ISE

You can create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the TACACS+ custom attributes that are associated with user roles, tasks, and virtual domains created in Cisco Evolved Programmable Network Manager.

For more information about Cisco ISE authorization profiles, see the information on managing authorization policies and profiles in the Cisco Identity Services Engine Administrator Guide.

To create an authorization profile for TACACS+ in Cisco ISE:

Before you begin

Make sure you have the complete list of the following Cisco Evolved Programmable Network Manager custom attributes for TACACS+. You will need to add this information to Cisco ISE in this procedure.

- Cisco Evolved Programmable Network Manager user roles and tasks—see Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+, on page 807
- Cisco Evolved Programmable Network Manager virtual domains—see Export the Cisco Evolved Programmable Network Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 821

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Work Center** > **Device Administration** > **Policy Elements**.

Step 3 From the left sidebar, choose **Results** > **TACACS Profiles**.

Step 4 In the **TACACS Profiles** page, click **Add**.

Step 5 From the **Access Type** drop-down list, choose **ACCESS_ACCEPT**.

Step 6 In the **TACACS Profiles** page, enter the name and description of the authorization profile.

Step 7 In the **Raw View Profile Attributes** area, paste in the complete list of TACACS+ custom attributes for:

- User roles, including the tasks
- Virtual domains

Note Be sure to add the Home Menu Access task. It is mandatory.

Step 8 Click **Submit**.

Configure an Authorization Policy in Cisco ISE

An authorization policy consists of a rule or a set of rules that are user-defined and produce a specific set of permissions, which are defined in an authorization profile. Based on the authorization profile, access requests to Cisco EPN Manager are processed.

There are two types of authorization policies that you can configure:

- Standard—Standard policies are intended to be stable and are created to remain in effect for long periods of time, to apply to a larger group of users, devices, or groups that share a common set of privileges.
- Exception—Exception policies are created to meet an immediate or short-term need, such as authorizing a limited number of users, devices, or groups to access network resources. An exception policy lets you create a specific set of customized values for an identity group, condition, or permission that are tailored for one user or a subset of users.

For more information about authorization policies, see the "Manage Authorization Policies and Profiles" chapter in the Cisco Identity Services Engine Administrator Guide.

To create an authorization policy in Cisco ISE:

Step 1 Log in to Cisco ISE as the admin user.

Step 2 Choose **Policy** > **Authorization**.

Step 3 In the **Standard** area, click the down arrow on the far right and select either **Insert New Rule Above** or **Insert New Rule Below**.

Step 4 Enter the rule name and choose identity group, condition, attribute, and permission for the authorization policy.

For example, you can define a user group as Cisco EPN Manager-System Monitoring-Group and choose this group from the Identity Groups drop-down list. Similarly, define an authorization profile as Cisco EPN Manager-System Monitoring-authorization profile and choose this profile from the Permissions drop-down list. Now, you have defined a rule where all users belonging to the Cisco EPN Manager System Monitoring identity group receive an appropriate authorization policy with system monitoring custom attributes defined.

Step 5 Click **Done**, and then click **Save**.

Create an Authentication Policy in Cisco ISE

Authentication policies define the protocols that Cisco ISE uses to communicate with Cisco EPN Manager, and the identity sources that it uses for authenticating users to Cisco EPN Manager. An identity source is an internal or external database where the user information is stored.

You can create two types of authentication policies in Cisco ISE:

- Simple authentication policy - In this policy, you can choose the allowed protocols and identity sources to authenticate users.

- Rule-based authentication policy - In this policy, you can define conditions that allow Cisco ISE to dynamically choose the allowed protocols and identity sources.

For more information about authentication policies, see the "Manage Authentication Policies" chapter in the Cisco Identity Services Engine Administrator Guide.

To create an authentication policy in Cisco ISE:

Step 1 Log in to Cisco ISE as the Super Admin or System Admin user.

Step 2 Choose **Policy** > **Authentication**.

Step 3 Choose the Policy Type as **Simple** or **Rule-Based** to create the required authentication policy.

Step 4 Enter the required details based on the policy type selected.

Step 5 Click **Save**.

Use Cisco ACS With RADIUS or TACACS+ for External Authentication

The Cisco Secure Access Control System (ACS) is no longer being sold. Please see the End-of-Sale and End-of-Life Announcement for the Cisco Secure Access Control System for more information. There will be no new development on the integration of Cisco Evolved Programmable Network Manager with Cisco ACS. The last date of support for the integration with ACS is scheduled for August 31, 2020, the date at which the ACS product will become obsolete.

Cisco Secure Access Control System (ACS) uses RADIUS and TACACS+ protocol for authentication, authorization, and accounting (AAA).You can integrate Cisco Evolved Programmable Network Manager with Cisco ACS to authenticate the Cisco Evolved Programmable Network Manager users using the RADIUS or TACACS+ protocol. When you use an external authentication, the details such as users, user roles, passwords, authorization profiles, authorization policies, and policy rules that are required for AAA must be stored and verified from the Cisco ACS database.

Complete the following tasks to use Cisco ACS with the RADIUS or TACACS+ protocol for external authentication:

Tasks to be completed to use Cisco ACS for external authentication	For information, see:
Make sure you are using a supported version of Cisco ACS	Supported Versions of Cisco ACS in Cisco Evolved Programmable Network Manager, on page 832
Add Cisco Evolved Programmable Network Manager as an AAA client in Cisco ACS	Add Cisco EPN Manager as a Client in Cisco ACS, on page 832
Create a user group in Cisco ACS	Create a User Group in Cisco ACS, on page 833
Create a user in Cisco ACS and add the user to the Cisco ACS user group	Create a User and Add the User to a User Group in Cisco ACS, on page 833

(If using RADIUS) Create an authorization profile for network access in Cisco ACS, and add the RADIUS custom attributes for user roles and virtual domains created in Cisco Evolved Programmable Network Manager. **Note** For RADIUS, you do not need to add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for RADIUS in Cisco ACS, on page 833
(If using TACACS+) Create an authorization profile for device administration in Cisco ACS, and add the TACACS+ custom attributes with user roles and virtual domains created in Cisco Evolved Programmable Network Manager. **Note** For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.	Create an Authorization Profile for TACACS+ in Cisco ACS, on page 834
Create an access service in Cisco ACS and define a policy structure for the access service.	Create an Access Service for Cisco EPN Manager in Cisco ACS, on page 835
Create an authorization policy rule in Cisco ACS, and map the authorization or shell profile based on the access type (network access or device administration).	Create an Authorization Policy Rule in Cisco ACS, on page 836
Configure a service selection policy in Cisco ACS and assign an access service to an incoming request.	Configure a Service Selection Policy in Cisco ACS, on page 836
Add Cisco ACS as a RADIUS or TACACS+ server in Cisco Evolved Programmable Network Manager.	Add a RADIUS or TACACS+ Server to Cisco EPN Manager, on page 824
Configure the RADIUS or TACACS+ mode on the Cisco Evolved Programmable Network Manager server.	Configure RADIUS or TACACS+ Mode on the Cisco EPN Manager Server, on page 825

Supported Versions of Cisco ACS in Cisco Evolved Programmable Network Manager

Cisco Evolved Programmable Network Manager supports Cisco ACS 5.*x* releases.

Add Cisco EPN Manager as a Client in Cisco ACS

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Network Resources** > **Network Devices** > **Network Devices and AAA Clients**.

Step 3 In the **Network Devices** page, click **Create**.

Step 4 Enter the device name and IP address of the Cisco EPN Manager server.

Step 5 Choose the authentication option as **RADIUS** or **TACACS+**, and enter the shared secret.

Note Ensure that this shared secret matches the shared secret you enter when adding the Cisco ACS server as the RADIUS or TACACS+ server in Cisco EPN Manager.

Step 6 Click **Submit**.

Create a User Group in Cisco ACS

Step 1 Log in to Cisco ACS as the admin user.
Step 2 From the left sidebar, Choose **Users and Identity Stores** > **Identity Groups**.
Step 3 In the **Identity Groups** page, click **Create**.
Step 4 Enter the name and description of the user group.
Step 5 Select a network device group parent for the user group.
Step 6 Click **Submit**.

Create a User and Add the User to a User Group in Cisco ACS

Step 1 Log in to Cisco ACS as the admin user.
Step 2 From the left sidebar, Choose **Users and Identity Stores** > **Internal Identity Stores** > **Users**.
Step 3 In the **Internal Users** page, click **Create**.
Step 4 Enter the required details.
Step 5 In the **Identity Group** field, click **Select** to choose a user group to assign the user to.
Step 6 Click **Submit**.

Create an Authorization Profile for RADIUS in Cisco ACS

You create authorization profiles to define how different types of users are authorized to access the network. For example, you can define that a user attempting to access the network over a VPN connection is treated more strictly than a user attempting to access the network through a wired connection.

When you create an authorization profile for device administration, you must add the RADIUS custom attributes that are associated with user roles, tasks, and virtual domains created in Cisco Evolved Programmable Network Manager.

Note For RADIUS, you can add the user role attributes without adding the task attributes. The tasks are automatically added with the user roles.

For more information about Cisco ACS authorization profiles and policies, see chapters on managing policy elements and access policies in the User Guide for Cisco Secure Access Control System.

To create an authorization profile for RADIUS in Cisco ACS:

Before you begin

Make sure you have the complete list of the following Cisco Evolved Programmable Network Manager custom attributes for RADIUS. You will need to add this information to Cisco ACS in this procedure.

- Cisco Evolved Programmable Network Manager user roles and tasks—see Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+, on page 807
- Cisco EPN Manager virtual domains—see Export the Cisco Evolved Programmable Network Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 821

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Policy Elements** > **Authorizations and Permissions** > **Network Access** > **Authorization Profiles**.

Step 3 Click **Create**.

Step 4 On the **General** tab, enter the name and description of the authorization profile.

Step 5 Click the **RADIUS Attributes** tab, and paste in the complete list of RADIUS custom attributes for:

- User roles
- Virtual domains

Note If you do add user tasks, be sure to add the Home Menu Access task. It is mandatory.

Step 6 Click **Submit**.

Create an Authorization Profile for TACACS+ in Cisco ACS

When you create an authorization profile for device administration, you must add the TACACS+ custom attributes that are associated with user roles and virtual domains created in Cisco Evolved Programmable Network Manager.

Note For TACACS+, you need not add the attributes for user tasks. They are automatically added based on the user roles.

For more information about Cisco ACS authorization profiles and policies, see chapters on managing policy elements and access policies in the User Guide for Cisco Secure Access Control System.

To create an authorization profile for TACACS+ in Cisco ACS:

Before you begin

Make sure you have the complete list of the following Cisco Evolved Programmable Network Manager custom attributes. You will need to add this information to Cisco ACS in this procedure.

- Cisco Evolved Programmable Network Manager user roles and tasks—see Export the Cisco EPN Manager User Group and Role Attributes for RADIUS and TACACS+, on page 807
- Cisco EPN Manager virtual domains—see Export the Cisco Evolved Programmable Network Manager Virtual Domain Attributes for RADIUS and TACACS+, on page 821.

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Policy Elements** > **Authorizations and Permissions** > **Device Administration** > **Shell Profiles**.

Step 3 Click **Create**.

Step 4 On the **General** tab, enter the name and description of the authorization profile.

Step 5 Click the **Custom Attributes** tab, and paste in the complete list of TACACS+ custom attributes for:

- User roles, including the tasks
- Virtual domains

Step 6 Click **Submit**.

Create an Access Service for Cisco EPN Manager in Cisco ACS

Access services contain the authentication and authorization policies for access requests. You can create separate access services for different use cases; for example, device administration (TACACS+), network access (RADIUS), and so on.

When you create an access service in Cisco ACS, you define the type of policies and policy structures that it contains; for example, policies for device administration, network access, and so on.

Note You must create access services before you define service selection rules, although you do not need to define the policies in the services.

To create an access service for Cisco EPN Manager requests:

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Access Policies** > **Access Services**.

Step 3 Click **Create**.

Step 4 Enter the name and description of the access service.

Step 5 Choose one of the following options to define a policy structure for the access service:

- **Based on service template**—Creates an access service containing policies based on a predefined template.
- **Based on existing service**—Creates an access service containing policies based on an existing access service. However, the new access service does not include the existing service's policy rules.
- **User selected service type**—Provides you the option to select the access service type. The available options are Network Access (RADIUS), Device Administration (TACACS+), and External Proxy (External RADIUS or TACACS+ servers).

Step 6 Click **Next**.

Step 7 Choose the authentication protocols that are allowed for the access service.

Step 8 Click **Finish**.

Create an Authorization Policy Rule in Cisco ACS

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Access Policies** > **Access Services** > **service** > **Authorization**.

Step 3 Click **Create**.

Step 4 Enter the name of the rule and then choose the rule status.

Step 5 Configure the required conditions for the rule.

For example, you can create a rule based on the location, device type, or user group that you have created.

Step 6 If you are creating an authorization policy rule for network access (RADIUS), choose the required authorization profile(s) to map to the authorization policy rule.

Alternatively, if you are creating an authorization policy rule for device administration (TACACS+), choose the required shell profile(s) to map to the authorization policy rule.

Note If you are using multiple authorization profiles or shell profiles, make sure you order them in priority.

Step 7 Click **OK**.

Configure a Service Selection Policy in Cisco ACS

A service selection policy determines which access service applies to an incoming request. For example, you can configure a service selection policy to apply the device administration access service to any access request that uses the TACACS+ protocol.

You can configure two types of service selection policy:

- Simple service selection policy—Applies the same access service to all requests.
- Rule-based service selection policy—Contains one or more conditions and a result, which is the access service that will be applied to an incoming request.

To configure a service selection policy:

Step 1 Log in to Cisco ACS as the admin user.

Step 2 From the left sidebar, choose **Access Policies** > **Access Services** > **Service Selection Rules**.

Step 3 If you want to configure a simple service selection policy, click the **Single result selection** radio button, and then choose an access service to apply to all requests.

Alternatively, if you want to configure a rule-based service selection policy, click the **Rule based result selection** radio button, and then click **Create**.

Step 4 Enter the name of the rule and then choose the rule status.

Step 5 Choose either **RADIUS** or **TACACS+** as the protocol for the service selection policy.

Step 6 Configure the required compound condition, and then choose an access service to apply to an incoming request.

Step 7 Click **OK**, and then click **Save Changes**.

Use SSO with External Authentication

To set up and use SSO (with or without a RADIUS or TACACS+ server), see these topics:

- Add the SSO Server, on page 837
- Delete SSO Server, on page 837
- Configure SSO Mode on the Cisco EPN Manager Server, on page 837

Cisco EPN Manager does not support localization on the SSO sign-in page.

Add the SSO Server

If you have deployed Cisco EPN Manager in a high availability environment where you have a primary and backup server, refer to the instructions in Configure an SSO Server in an HA Environment, on page 887.

Cisco EPN Manager can be configured with a maximum of three AAA servers.

Step 1 Choose **Administration** > **Users** > **AAA**, then choose **Servers**. Select the **SSO** tab. From this window, you can add, edit settings, and delete a new SSO server.

Step 2 Click the  icon.

Step 3 Enter the SSO information. The maximum number of server retries for an SSO server authentication request is nine.

Step 4 Click **Save**.

Note You can also add the Cisco EPN Manager server you are using as an SSO server. To add, select the **Add self as SSO** checkbox.

Delete SSO Server

You can delete the SSO server that is added to Cisco EPN Manager. To delete the SSO server:

Step 1 Choose **Administration** > **Users** > **AAA**, then choose **Servers**. Select the **SSO** tab.

Step 2 Select the servers that you want to delete.

Step 3 Click the checkbox next to the SSO server and click  . The Delete dialog box opens. Click **Delete** to confirm.

Configure SSO Mode on the Cisco EPN Manager Server

The SSO functionality distributes CA certificate when the SSO server is added to the SSO client.

Cisco EPN Manager supports CA and self-signed certificates as long as the Common Name (CN) field of the certificate contains the Fully Qualified Domain Name (FQDN) of the server on the SSO client and SSO server.

The server must be capable of name resolution from the IP address to FQDN. In addition, the hostname must match the left-most component of the FQDN. SSO requires accurate DNS configuration. You must define the DNS with fully qualified domain name (FQDN). For example, the nslookup command and expected data when configuring DNS with FQDN is:

```
hostname CUSTOMER_HOSTNAME
nslookup CUSTOMER_HOSTNAME
Server:...
Address:...
Name: CUSTOMER_HOSTNAME.example.com
Address:....
```

For SSO operation, Cisco EPN Manager requires that the SSL/TLS certificate holds the FQDN in the CN field. To verify that the certificate used by your Cisco EPN Manager server has the FQDN in the CN field, use your browser to view the certificate. If the certificate does not contain the FQDN in the CN field, you must regenerate the certificate and redistribute it to all users that have the old certificates.

Note If you are using this procedure to configure SSO but are using local authentication, choose **Local** in Step 2.

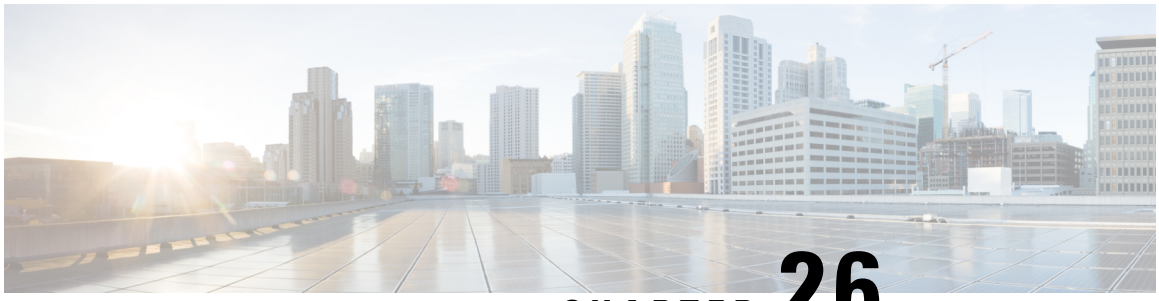
Step 1 Choose **Administration** > **Users** > **AAA**, then choose **SSO Settings**.

Step 2 Choose which **SSO Server AAA Mode** you want to use. You can select only one at a time.

Step 3 Select/de-select **Enable Single Sign-Out** checkbox.

Step 4 Choose a time span from the **Ticket Granting Ticket Timeout** drop-down.

Step 5 Click **Save All Changes**.



CHAPTER 26

Fault Management Administration Tasks

Note Advanced users can also use the Cisco EPN Manager Representational State Transfer (REST) API to access device fault information. For information on the API, click at the at the top right of the Cisco EPN Manager window, then choose **Help** > **API Help**.

Event Receiving, Forwarding, and Notifications

Cisco EPN Manager processes syslogs and SNMPv1, v2, and v3 traps that it receives from devices. The server automatically listens for these events on UDP port 162. You do not have to perform any event listening configuration on the server, but you do have to configure devices to forward traps and syslogs to Cisco EPN Manager on the appropriate port.

Notifications are forwarded in SNMPv2 or SNMPv3 format. They are also forwarded to email recipients when you setup corresponding Notification Policies. If you are adding a notification receiver with the notification type UDP, the receiver you add should be listening to UDP on the same port on which it is

configured. Only INFO level events are processed for the selected category and alarms are processed with critical, major, minor and warning levels.

Note Notification receivers using SNMPv3 format must have unique usernames. If two or more notification receivers have the same username but different passwords, one of them will not function.

Cisco EPN Manager can forward alarms and events that are generated by the processing of received syslogs, traps, and TL/1 alarms to northbound notification receiver. Alarms of any severity can be forwarded, but only events with INFO severity can be forwarded. Information can be forwarded in :

- E-Mail format. See Configure Default Settings for E-Mail Notifications, on page 847
- SNMP trap format. See Forward Alarms and Events as SNMP Trap Notifications, on page 846

You can also use the SNMP trap notification mechanism to forward SNMP traps that indicate server problems.

Alerts and events are sent as SNMPv2.

User Roles and Access Permissions for Configuring Alarm Notification Settings

This table describes the user roles and access permissions for configuring notification destination and creating customized notification policies.

Note Ensure that you enable the following Task Permissions for any user roles to view, create, and edit notification destination and notification policy:

- Notification Policies Read-Write Access under Alerts and Events
- Virtual Domains List

For more information, see View and Change the Tasks a User Can Perform, on page 794.

User Role	Access Permission
Root user with root domain	View, create, delete and edit notification destination and notification policy.
Root user with non-root domain	View notification destination and notification policy.
Admin user with root domain	View, create, delete and edit notification destination and notification policy.
Super user with root domain	View, create, delete and edit notification destination and alarm notification policy.
System monitoring user with root domain	View notification destination and notification policy.
Config manager with root domain	View notification destination and notification policy.

User Role	Access Permission
Admin user with non-root domain	View notification destination and notification policy created under their respective virtual domain.
Super user with non-root domain	View notification destination and notification policy created under their respective virtual domain.
System monitoring user with non-root domain	View notification destination and notification policy created under their respective virtual domain.
Config manager with non-root domain	View notification destination and notification policy created under their respective virtual domain.

Points to Remember While Adding a New Notification Policy

The following table lists few points you must remember when adding a new notification policy.

Category selected under Notification Policy Page	Points to Remember
Email	• Each virtual domain must have a unique Contact Name and email address (email recipient). • Email recipients can be added, modified, and deleted only from the ROOT-DOMAIN. • Same email address can be associated with multiple virtual domains. • Cisco EPN Manager does not use the Telephone Number, Cell Number, and Postal Address details for sending alarm notifications.
Trap Receiver	• Contact Name is unique for each trap receiver. • Trap receivers can be added, modified, and deleted only from the ROOT-DOMAIN. Trap receivers are applicable only in ROOT-DOMAIN. • Only North Bound trap receivers can receive alarms/events forwarded from the Notification Policy engine. • Guest-Access trap receivers will receive only alarms related to guest clients.

Category selected under Notification Policy Page	Points to Remember
Notification Policy	• Each notification policy consists of the following criteria: alarm categories, alarm severities, alarm types, device groups, notification destinations, and time range. • Each notification policy is associated with a unique virtual domain. • While selecting the required conditions, you can drill down the tree view drop-down list and select the individual categories (for example, Switches and Routers) and the severity (for example, Major). You can further select the specific Alarm types (for example, link down). • Alarms that match the criteria in a policy are forwarded to the respective notification destinations. • If an alarm is matched against multiple policies in the same virtual domains and these policies have the same destinations, only one notification is sent to each destination. • If the virtual domain associated with a notification policy is deleted, no alarm will match this policy. Though, this notification policy will be listed in the main Notification Policy page, you cannot modify or view the details of this notification policy. However, you can delete this policy. • If one or more device groups specified in a policy is deleted, no alarm will match this policy. Though, this notification policy will be listed in the main Notification Policy page, you cannot modify or view the details of this notification policy. However, you can delete this policy. • Alarms that are suppressed due to an existing alarm policy will not be forwarded to the notification destinations. • If a notification policy that includes both system and non-system category alarms in the rule criteria, you must select the device group(s) for the non-system category alarms. • The alarms generated in the specified duration alone are sent to the notification destination. For example, if you specify the duration as 8:00 to 17:00, the alarms will be notified from 8.00 a.m. to 5.00 p.m.

Configure Alarms Notification Destination

You can configure the email notification and Northbound trap receiver settings to notify the alarms generated by Cisco EPN Manager.

Step 1 Choose **Administration** > **Settings** > **System Settings** > **Mail and Notification** > **Notification Destination**.

Step 2 Click the  icon to create a new notification destination.

Step 3 To configure Email Destination, do the following:

a) From the **Select Contact Type** drop-down list, choose **Email**.
b) Enter the **Contact Name** in the text box.
c) Enter a valid email ID in the **Email To** text box.
The email is sent to the email ID entered in the **Email To** field.
d) Enter the **Contact Full Name**.
e) Enter the **Telephone Number**, **Mobile Number**, and **Postal Address**.
f) Click **Save**.

Step 4 To configure a Northbound trap receiver using IP Address, do the following:

a) From the **Select Contact Type**, choose **Northbound Trap Receiver**.
b) Select the **IP Address** radio button, and enter the **IP Address** and **Server Name**.
c) Enter the **Port Number**, and choose the **SNMP Version**.
d) If you choose the **SNMP Version** as **v2c**, enter the **Community** settings as required.
e) If you choose the **SNMP Version** as **v3**, enter the **Username**, **Mode**, **Auth. Type**, **Auth. Password**, **Confirm Auth. Password**, **Privacy Type**, **Privacy Password**, and **Confirm Privacy Password**.
f) Choose the required **Receiver Type** and **Notification Type**.
g) Click **Save**.

Step 5 To configure a Northbound trap receiver using DNS, do the following:

a) From the **Select Contact Type**, choose **Northbound Trap Receiver**.
b) Select the **DNS** radio button and enter the **DNS Name**.
c) Enter the **Port Number**, and choose the **SNMP Version**.
d) If you choose the **SNMP Version** as **v2c**, enter the **Community** settings as required.
e) If you choose the **SNMP Version** as **v3**, enter the **Username**, **Mode**, **Auth. Type**, **Auth. Password**, **Confirm Auth. Password**, **Privacy Type**, **Privacy Password** and **Confirm Privacy Password**.
f) Choose the required **Receiver Type** and **Notification Type**.
g) Click **Save**.

Note

- If you choose the **Receiver Type** as **Guest Access**, Cisco EPN Manager will not forward the alarms to the Northbound trap receiver using the notification policy. The Guest Access receiver receives only guest-client related events. The notification policy uses only Northbound trap receivers. Make sure that you use the same Engine ID and same auth and priv passwords when configuring the external SNMPv3 trap receiver.
- While updating the Notification Destination Trap Receiver, the operational status shows that the previous Trap Receiver status until the status is updated by the next polling.
- You can also navigate to Notification Policies page by choosing **Monitor > Monitoring Tools > Notification Policies** .
- If recipient email id is configured in multiple Notification policies, alarm will be forwarded only once to the email id, when condition matches.
- You will not be allowed to delete Notification Destinations which are associated with Notification Policies.

Delete a Notification Destination

Follow this procedure to delete a Notification Destination.

Before you begin

You cannot delete a Notification Destination which is associated with a Notification Policy. Ensure that you have disassociated the Notification Destination from the Notification Policy. To do this, edit the Alarm Notification Policy and assign a different Notification Destination. See Customize Alarm Notification Policies, on page 844 for more information.

Note If a Notification destination is associated with multiple Notification policies, ensure that you have disassociated the Notification destination from all associated Notification policies.

Step 1 Navigate to **Administration** > **Settings** > **System Settings** > **Mail and Notification** > **Notification Destination**

Step 2 Select the Notification Destination you want to delete by selecting the check box next to it.

Step 3 Click the Delete icon.

Customize Alarm Notification Policies

You can add a new alarm notification policy or edit an existing alarm notification policy to send notifications on specific alarms of interest that are generated on particular device groups, to specific email recipients, northbound trap receivers, and restconf receivers.

Note The restconf option is available only if the user enables the restconf option in **Administration > Settings > System Settings > Alarms and Events > Alarm And Events > Alarm other Settings**.

Step 1 Choose **Administration > Settings > System Settings > Alarms and Events> Alarm Notification Policies**. To add a new alarm notification policy, do the following:

a) Click the **Add** icon.

b) Choose the severity, category, and event condition for which the notifications must be triggered. By default all the severity types, categories, and conditions are selected.

c) Click **Next** and choose the device groups for which you want the alarm notifications to be triggered.

The alarm notifications are triggered only for the device groups that you select.

For instance, if you select the **User Defined** device group type, then the alarm notification is triggered for all the configured user defined device groups. Similarly, if you select both the **User Defined** and **Locations** device group types, then the alarm notifications are triggered for all the configured user defined and location device groups.

Select the desired device group type to abstain from receiving insignificant alarm notifications from other device groups.

If you choose only system category alarms in the previous step, a message "Device Groups are not applicable when only 'System' based alarms are selected" is displayed under the **Device Group** tab. However, if you choose a nonsystem category alarm, you must select at least one device group.

d) Click **Next** and choose the required destination in the **Notification Destination** page.

e) Click  icon and enter the required details in the **Add Destination** window. You can choose either the **Email** or **Northbound Trap Receiver** or **Restconf** option under **Select Contact Type**.

f) Click **Next** and enter the **Name** and **Description** for the alarm notification policy in the **Summary** page.

g) Click **Save**.

Note "Interface" is a reserved word and hence don't use it as the name for Alarm Notification Policy.

Step 2 To edit an alarm notification policy, do the following:

a) Choose the policy and click the  icon. The **Notification Policies** wizard appears.

b) Choose the **Conditions**, **Device Groups**, and **Destination** as explained in Step 1.

c) Click **Save**.

Convert Old Email and Trap Notification Data to New Alarm Notification Policy

The email and trap notification data created in previous Cisco Evolved Programmable Network Manager releases is converted into a new alarm notification policies while upgrading or migrating Cisco Evolved Programmable Network Manager from previous release to the latest version.

The migrated alarm notification policies can be viewed in the Alarms and Events Notification Policies pages.

The following Alarm categories are supported in Cisco Evolved Programmable Network Manager:

- Application Performance
- Change Audit
- Clients
- Compute Servers

- Context Aware Notifications
- Controller
- Generic
- Mobility Service
- Nexus VPC switch
- Performance
- SE Detected Interferers
- Security
- Switches and Routers
- System

The following Alarm categories are not supported in Cisco Evolved Programmable Network Manager:

- Adhoc Rogue
- AP
- Autonomous AP
- Cisco UCS Series
- Coverage Hole
- Mesh links
- Routers
- Rogue AP
- RRM
- Switches and Hubs
- Third Party AP
- Third Part Controller
- Wireless Controller

To edit the migrated alarm notification polices, see Customize Alarm Notification Policies, on page 844.

Forward Alarms and Events as SNMP Trap Notifications

Cisco Evolved Programmable Network Manager can forward alarms and events in EPM-NOTIFICATION-MIB format as an SNMPv2c and SNMPv3 trap notifications. You can specify:

- A specific alarm or event category, such as **System** for internal server SNMP traps.
- Alarms of a specific severity. Only INFO *events* are forwarded; you cannot specify other severities for events.

See Configure Alarms Notification Destination, on page 843 for more information.

Configure Default Settings for E-Mail Notifications

If you have not configured the mail server, perform the instructions in Set Up the SMTP E-Mail Server, on page 767. Otherwise notifications will not be sent.

You can configure certain default settings that are applied across all alarm and event e-mail notifications. These settings can be overwritten when users configure individual notifications and receivers.

By default, the email subject line will include the alarm severity and category. The following settings are also available but are disabled by default.

- Subject line—Include the prior alarm severity or add custom text. Alternatively you can replace all of the subject line with custom text.
- Body of the email—Include custom text, the alarm condition, and a link to the alarm detail page.
- Secure message mode—Enabling this mode masks the IP address and controller name.

To enable, disable, or adjust these settings, choose **Administration** > **Settings** > **System Settings**, then **Alarms and Events** > **Alarms and Events**. Make your changes in the **Alarm Email Options** area.

Specify Alarm Clean Up, Display, and Email Options

The **Administration > Settings > System Settings > Alarms and Events** page enables you to specify when and how to clean up, display, and email alarms.

Step 1 Choose **Administration > Settings > System Settings > Alarms and Events > Alarms and Events**.

Step 2 Modify the **Alarm and Event Cleanup Options**:

- Delete cleared non-security alarms after—Enter the number of days after which non-security alarms are deleted. Non-security alarms include all alarms that do not fall under the Security or Adhoc Rogue categories.
- Delete cleared security alarms after—Enter the number of days after which Security and Adhoc Rogue alarms are deleted.
- Delete all (active & cleared) alarms after—Enter the number of days after which active and cleared alarms are deleted.
- Delete all events after—Enter the number of days after which all events are deleted.

The maximum limit is 8000000 events or the number of days specified, whichever is lower.

Step 3 Modify the **Syslog Cleanup Options**:

- Delete all Syslogs after—Enter the number of days after which all aged syslogs are deleted.
- Max Number of Syslog to Keep—Enter the number of Syslogs that needs to be maintained in the database.

Step 4 Modify the **Alarm Display Options** as needed:

- Hide acknowledged alarms—When this check box is selected, Acknowledged alarms do not appear in the Alarm page. This option is enabled by default. Emails are not generated for acknowledged alarms, regardless of severity change.

- Hide assigned alarms—When this check box is selected, assigned alarms do not appear in the Alarm page.
- Hide cleared alarms—When this check box is selected, cleared alarms do not appear in the Alarm page. This option is enabled by default.
- Show only Active Alarms in the Alarms tab - When this check box is selected, only Active Alarms appear in the Alarms list under Alarms tab.
- Add device name to alarm messages—Select the check box to add the name of the device to alarm messages.

Changes in these options affect the Alarm page only. Quick searches for alarms for any entity display all the alarms for that entity, regardless of the alarm state.

Step 5 Modify the alarm Failure Source Pattern:

- Select the category that you need to customize and click **Edit**.
- Select the failure source pattern in the options available and click **OK**.
- Select the category for which you want to customize the separator and click **Edit Separator**. Select one of the options available, then click **OK**.

The alarms generated for the selected category have the customized patterns set by you. For example, if you select the Clients category and edit the separator as **#**, then for any supported client alarm that is generated (**Monitor > Monitoring Tools > Alarms and Events**), the Failure Source column for that alarm will be *MACaddress #Name*.

Note Failure Source is not supported for custom traps, syslog generated events, and custom syslog translation.

Step 6 Modify the **Alarm Email Options**:

- Add Cisco EPN Manager address to email notifications—Select this check box to add the Cisco EPN Manager address to email notifications.
- Include alarm severity in the email subject line—Select this check box to include alarm severity in the email subject line. This option is enabled by default.
- Include alarm Category in the email subject line—Select this check box to include alarm category in the email subject line. This option is enabled by default.
- Include prior alarm severity in the email subject line—Select this check box to include prior alarm severity in the email subject line.
- Include custom text in the email subject line—Select this check box to add custom text in the email subject line. You can also replace the email subject line with custom text by selecting the Replace the email subject line with custom text check box.
- Include custom text in body of email—Select this check box to add custom text in the body of email.
- Include alarm condition in body of email—Select this check box to include alarm condition in the body of email.
- Include alarm application category data in body of email—Select this check box to include alarm category in the body of email.
- Add link to Alarm detail page in body of email—Select this check box to add a link to the Alarm detail page in the body of email.
- Enable Secure Message Mode—Select this check box to enable a secure message mode. If you select the Mask IP Address and Mask Controller Name check boxes, the alarm emails are sent in secure mode, where all the IP addresses and controller names are masked.

- Email Send Interval—Specify the time interval during which the email has to be sent.

Note Cisco EPN Manager sends alarm notification email for the first instance of an alarm and the subsequent notification is sent only if the alarm severity is changed.

Step 7 Modify the **Miscellaneous Settings**:

- **Controller License Count Threshold**—Enter a threshold percentage. An alarm is triggered if the number of access points connected to a controller reaches the specified rate of the licenses available on the controller. For example, if a controller is configured with 100 access point licenses and 80% threshold, an alarm will be triggered when the number of access points connected to a controller exceeds 80.
- **Enable AP count threshold alarm**—Select this check box to enable the AP count for threshold alarms.
- **Controller Access Point Count Threshold**—Enter a threshold percentage. An alarm is triggered if the number of access points connected to a controller reaches the maximum number of access points supported by the controller. For example, if a controller supports a maximum of 6000 access points and threshold is configured as 80%, an alarm will be triggered when the number of access points connected to the controller exceeds 4800.
- **Suppress Interface Optical SFP TCAs in Admin Down State**—Selecting this check box prevents optical SFP TCAs to be raised for interfaces in the Admin Down state.
- **Enable Service Impact Analysis**—Selecting this check box enables the service impact analysis.
- **Enable creation of subtrees from a correlation tree when root cause of the tree clears**—When the root cause of a correlation tree clears, subtrees of this correlation tree are created, where each subtree has an uncleared root cause, selecting this check box enables this feature.
- **Enable alarms from interface status polling**—If this check box is selected, LinkDown alarms will be raised and cleared by polling the interface status of Ethernet and Bundle Interfaces.
- **Enable alarm generation based on EPNM inventory collection**—Cisco EPN Manager uses the inventory status of entities to raise and clear certain alarms. This mechanism acts as a backup for syslogs and traps, which may be lost or missing (due to the device not generating them, lost in network, and so on).
- **Enable User Defined Field**—If this setting is enabled, PRODUCT_NAME and PRODUCT_ID are conditionally populated for Hardware Alarms in the Alarms list under the **Alarms** tab. This setting does not affect existing alarms and does not apply on previously raised alarms. This setting is disabled by default.
- **Enable Event Throttle**—If this check box is selected, Cisco EPN Manager proactively drops events if the event count exceeds the threshold count (by default, more than 3600 events raised within 1 hour) for a device. See Customize Event Throttle per Device, on page 855 for more information.
- **Enable Alarms Cross Launch to SVO**—Select this check box to enable the cross launch to SVO nodal craft from Alarms table (**Monitor** > **Monitoring Tools** > **Alarms and Events**).

  Note To avoid entering login credentials each time you navigate to SVO UI, enable Single Sign-on (SSO) from Cisco EPN Manager to SVO nodal craft. See Enable Single Sign-on (SSO) from Cisco EPN Manager to SVO UI , on page 50 for more information.
- **Enable Transient Condition Alarms**—If this check box is selected, then the Cisco EPN Manager processes transient events as alarms and displays these events in the **Alarms** table. By default, this check box is not checked.
- **Enable Network Alarms View**—Selecting this option adds the tab **Network Alarms** under the **Alarms** tab. The **Network Alarms** tab lists all network impacting alarms. By default, this option is disabled.

- **Enable Notification Policy based filter for NBI WebSocket's Client**—Select this check box to enable restconf in the alarm notification policies to add the northbound WebSocket destination.
- **Max no. of Netconf Session Retry**—Enter the number of Netconf session attempts to connect and handle SVO faults.
- **Netconf Session Retry Interval**—Enter the time interval between retry attempts (in seconds), and to enable the Netconf session to handle any SVO faults.
- **Enable Device UDF to be sent in notifications**—Select this check box to enable alarm notifications for device UDFs.
- **Enable Not Alarmed (NA) Condition Alarms**—Select this check box to avoid events to be processed as alarms for optical devices.
- **Enable Alarms & Events Replay support for SVO Devices**—Select this check box to enable Netconf replays for SVO devices. This replays events that were lost during network connection failure, SVO switch over, device down time, or any other connection failure.
- **Duration for the Alarms & Events Replay for SVO Devices**—Enter the maximum time duration that you need for the alarms and events to be synced. The default option is 720 minutes or 12 hours. We recommend that you avoid entering a large time duration for this field.
- **Enable to suppress Alarms and Events for card/port in maintenance mode**—Select this check box to suppress any traps, alarms, or syslogs generated by a line card/port in maintenance mode.

Step 8 For **Alarm Manager Settings**, see Configure Alarm Manager in Cisco IOS XR Devices, on page 851.

Step 9 Click **Save**.

Configure Global Display and Search Settings for Acknowledged, Cleared, and Assigned Alarms

The following table lists some display options for acknowledged, cleared, and assigned alarms. These settings *cannot* be adjusted by individual users (in their display preferences) because, for very large systems, a user could make a change that will impact system performance.

Other settings shown on the Alarms and Events page can be adjusted by users, but you can set the global defaults here. For information on those settings, see these topics:

- Configure Default Settings for E-Mail Notifications
- Alarm, Event, and Syslog Purging, on page 786

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarms and Events**.

Step 2 Under the Alarm Display Options area, enable or disable these settings, as desired:

Alarm Display Options	Description	Does setting also affect search results?

Hide acknowledged alarms	Do not display Acknowledged alarms in the Alarms list or include them in search results	Yes
Hide assigned alarms	Do not display assigned alarms in the Alarms list or in search results	Yes
Hide cleared alarms	Do not display cleared alarms in the Alarms list or in search results For example, if there are 3900 cleared alarms out of 4000 alarms, enabling this setting will display 100 uncleared alarms in the Alarms list under **Alarms** > **Showing Active Alarms**. **Note** Cleared alarms remain viewable under the **Cleared Alarms** tab.	No
Show only Active Alarms in Alarms tab	Display only Active Alarms in the Alarms list under **Alarms** tab. For example, if there are 3900 cleared alarms out of 4000 alarms, enabling this setting will display the latest 4000 uncleared alarms in the Alarms list under **Alarms** > **Showing Active Alarms**. **Note** Cleared alarms remain viewable under the **Cleared Alarms** tab.	No
Add device name to alarm messages	Include device name in e-mail notifications	No

Step 3 To apply your changes, click **Save** at the bottom of the Alarms and Events window.

Configure Alarm Manager in Cisco IOS XR Devices

As part of reliable alarming, Cisco EPN Manager polls the Alarm Manager in Cisco IOS XR devices for any outstanding alarms or events.

Note Alarm Manager support is limited to Cisco IOS XR devices NCS 10xx, NCS 40xx and NCS 55xx only.

Follow this procedure to enable or disable the Alarm Manager from Cisco EPN Manager GUI.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarms and Events**.

Step 2 Under **Alarm Manager Settings**, select the device type to enable or disable the Alarm Manager as required.

Note By default, Alarm Manager is enabled for all the device types listed under the **Alarm Manager Settings** area.

Step 3 Click **Save** to apply your changes.

Step 4 Click **Save** at the bottom of the Alarms and Events window.

If the Alarm Manager is enabled, Cisco EPN manager polls the device every 5 minutes. You cannot change this polling interval. All alarms raised by Alarm Manger are displayed in the list under **Alarms** tab in **Monitor** > **Monitoring Tools** > **Alarms and Events** page. You cannot modify the Severity or Clear or Delete the alarms raised by Alarm Manager in this list. The source of the alarm is displayed as "Synthetic_Event" for alarms raised by the Alarm Manager,

If the Alarm Manger is disabled, all the alarms previously raised by Alarm Manager are cleared. Cisco EPN Manager will no longer poll the device but continues to receive alarms directly from the device. All PKT-INFRA-FM alarms will be listed under the **Events** tab in **Monitor** > **Monitoring Tools** > **Alarms and Events** page.

Configure Alarm Resync in Cisco IOS XE Devices

The alarm resync feature, based on the "show facility" command is part of reliable alarming for Cisco IOS XE devices. This feature is supported from software version 16.6.6vS and 16.9.1 in Cisco NCS 42xx devices. You can enable or disable alarm resync by modifying the `/conf/fault/ncs42xx/resources/NCS42xxAlarmManager.properties` file.

When the alarm resync is enabled, the alarms received from the device are displayed under Alarms tab in **Monitor** > **Monitoring Tools** > **Alarms and Events** page. You cannot modify the Severity or Clear or Delete these alarms through Cisco EPN Manager.

Note The alarm resync feature is supported only for DSX, SONET and select system alarms. Refer to Cisco Evolved Programmable Network Manager Supported Syslogs for more information.

The following procedure lists the steps to enable or disable the alarm manager in Cisco NCS 42xx devices.

Step 1 Open a CLI session with the Cisco EPN Manager server. See Connect via CLI, on page 752 for more information.

Step 2 Open the `/conf/fault/ncs42xx/resources/NCS42xxAlarmManager.properties` file.

Step 3 Modify `shfacilityenabled`, `resyncperiodmillis`, and `pollerperiodmillis` as required.

- `shfacilityenabled` - flag to enable or disable Alarm Manager. Setting this flag to true will enable the alarm resync. By default, this value is set to true. System restart is not required when you change this value.
- `resyncperiodmillis` - polling interval to poll the device. You can modify this value as desired. Default value is 600000 milliseconds or 10 minutes. System restart is required for this change to take effect.
- `pollerperiodmillis` - poller which updates the device list to poll for alarm manager. You can modify the value as desired. Default value is 3600000 milliseconds or 1 hour. System restart is required for this change to take effect.

Configure Alarm Profiling in Cisco IOS XE Devices

Cisco EPN Manager supports alarm profiling for Cisco IOS XE devices. Set `alarmprofileEnabled` to `true` for Cisco EPN Manager to reflect the alarm profiling changes. To do this:

Step 1 Open a CLI session with the Cisco EPN Manager server. See Connect via CLI, on page 752 for more information.

Step 2 Open the `/conf/fault/ncs42xx/resources/NCS42xxVersion.properties` file.

Step 3 Set `alarmprofileEnabled` to `true` and save your changes. By default, the `alarmprofileEnabled` is enabled.

Note If `alarmprofileEnabled` is set to false, Cisco EPN Manager does not reflect the alarm profiling changes.

Change Alarm Severity Levels

Each alarm in Cisco EPN Manager has a severity. The alarm severity is determined by the most severe event associated to the alarm. You can adjust the severity for alarms by changing the severity for newly generated events.

Note For alarms that are related to Cisco EPN Manager system administration, such as high availability, refer to Customize Server Internal SNMP Traps and Forward the Traps, on page 777.

For entsensor alarms, you must not change the default severity using the default severity configuration page.

You can change the severity level for network- and device-level alarms in two ways:

- Threshold-crossing alarms generated by optical, Carrier Ethernet, device health, or interface health monitoring policies—change the settings in the relevant monitoring policy. See Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 234.
- Specific alarms—use the procedure in this section.

Step 1 Choose **Administration** > **System Settings**, then choose **Alarms and Events** > **Alarm Severity and Auto Clear**.

Step 2 Expand the categories available under the **Alarm Condition** column, or search for the Alarm Condition you want by entering all or part of the event text in the **Alarm Condition** search field just below the column heading.

Step 3 Select the events and set their new severity.

a) Check the event's checkbox.

b) Choose a severity level from the **Severity** drop-down list and click **Save**.

Note For a **Custom Syslog**, the **Severity Level** changed under the **Alarm Severity and Auto Clear** page will not be reflected under the **Alarms and Events** > > **Syslog** tab.

Customize the Troubleshooting Text for an Alarm

You can associate troubleshooting and explanatory information with an alarm so that users with access to the Alarms and Events tables will be able to see it. Use this procedure to add or change the information that is displayed in the popup window.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarm Severity and Auto Clear**.

Step 2 Select and alarm, then click **Recommended Action**.

Step 3 Add or change the content in the **Explanation** and **Recommended Actions** fields, then click **Save**. To revert to the default text, click **Reset** and **Save**.

Change Alarm Auto-Clear Intervals

You can configure an alarm to clear automatically after a specific period. This is helpful in cases, for example, where there is no clearing event. Auto clearing an alarm will not change the severity of the alarm's correlated events.

You can set the auto clear duration in intervals of 5 minutes, up to a duration of 55 minutes. Beyond this time, you can set an interval in multiples of an hour or 60 minutes.

Note

- When you enable alarm auto clear, at times there may be a delay in clearing the created alarms.
- When you set an auto clear interval that is less than an hour, it may affect the system performance.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarm Severity and Auto Clear**.

Step 2 Expand the categories available under the **Event Types** column, or search for an event type by entering all or part of the event text in the **Event Types** search field below the column heading.

Step 3 To change the auto clear duration, select one or more events and click the **Alarm Auto Clear** button.

Step 4 Click **Ok** to save the auto clear time duration.

Change the Information Displayed in the Failure Source for Alarms

When an alarm is generated, it includes information about the source of the failure. Information is presented using a specific format. For example, performance failures use the format *MACAddress***:***SlotID*. Failure sources for other alarms may include the host name, IP address, or other properties. Adjust the properties and separators (a colon, dash, or number sign) that are displayed in the alarm's failure source using the following procedure.

Step 1 Choose **Administration** > **Settings** > **System Settings**, then choose **Alarms and Events** > **Alarms and Events**.

Step 2 In the Failure Source Pattern area, select the alarm category you want to customize.

Step 3 Adjust the failure source format as follows:

- To customize the *properties* that are displayed, click **Edit**, select the properties, then click **OK**. If a property is greyed-out, you cannot remove it.
- To customize the *separators* that are displayed between the properties, click **Edit Separator**.

Step 4 To apply your changes, click **Save** at the bottom of the Alarms and Events settings window.

Customize Event Throttle per Device

Cisco EPN Manager proactively drops events once the number of events raised by a device exceeds a threshold value. The event processing resumes once a lower threshold is reached.

By default, Cisco EPN Manager proactively drop events from a device if there are more than 3600 events raised within 1 hour. The event processing resumes once the event count comes down to 3000.

To modify the default threshold values:

Before you begin

To enable this feature:

1. Navigate to **Administration > Settings > System Settings > Alarms and Events > Alarms and Events**.
2. Select the **Enable Event Throttle** check box.

Step 1 Open a CLI session with the Cisco EPN Manager server (see Connect via CLI, on page 752 for more information).

Step 2 Open the `/conf/fault/cep/EventThrottleRules.xml` file.

Step 3 Specify the required values in the following rules:

- `Add_Suppress_Event_Based_On_Count_Per_Device_Rule`

  - threshold count at which Cisco EPN Manager proactively drops events raised by the device. By default, this value is 3600.
- `Remove_Suppress_Event_Based_On_Count_Per_Device_Rule` - threshold count at which Cisco EPN Manager resumes processing the events. The default value is 3000.

Event Throttle for the System

Cisco EPN Manager checks for network congestion by setting an event throttle to check events at the system level.

If the queue occupancy in the network increases beyond 60%, it starts to drop events. In such a scenario, you see the following message:

The system event processing queue has reached the configured upper threshold value. Please check for sustained high network event rate to avoid dropping of events.

If the queue occupancy in the network reaches its complete capacity, you see the following message:

The system event processing queue is full and oldest events from the queue will be dropped. Please find the details of the dropped events in assurance_fault.log.

In both the scenarios, we recommend that you check for network outage or factors responsible for an excessive amount of incoming network events.

Note that the upper threshold percentage value is set at 60% of the queue capacity after which an alarm gets generated. When the system reaches the lower threshold percentage of 30%, the alarm gets cleared.

Change the Behavior of Expedited Events

When Cisco EPN Manager receives a configuration change event from a device, it waits for a certain time interval before starting inventory collection, in case other related events are sent. This prevents multiple collection processes from running at the same time. This is called the *inventory collection hold off time* and is set to 10 minutes by default. This setting is controlled from the Inventory system settings page (**Administration** > **Settings** > **System Settings** > **Inventory**).

The following events are processed by Cisco EPN Manager within the default time interval of 10 minutes:

Type	Supported Events
Link	LINK-3-UPDOWN
Card Protection	CARD_PROTECTION-4-PROTECTION CARD_PROTECTION-4-ACTIVE
VLAN	PORT_SECURITY-6-VLAN_REMOVED PORT_SECURITY-6-VLAN_FULL
ICCP SM	L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION L2-L2VPN_ICCP_SM-4-REMOTE_CORE_ISOLATION_CLEAR L2-L2VPN_ICCP_SM-3-CONFIG_LOCAL_ERROR L2-L2VPN_ICCP_SM-3-CONFIG_REMOTE_ERROR L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION L2-L2VPN_ICCP_SM-4-LOCAL_CORE_ISOLATION_CLEAR L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_FAILURE L2-L2VPN_ICCP_SM-4-PEER_REACHABILITY_CLEAR L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE L2-L2VPN_ICCP_SM-4-REMOTE_ACCESS_MAIN_PORT_FAILURE_CLEAR INFRA-ICCP-5-ISOLATION INFRA-ICCP-5-ISOLATION_CLR INFRA-ICCP-5-NEIGHBOR_STATE_UP INFRA-ICCP-5-NEIGHBOR_STATE_DOWN INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_UP INFRA-ICCP-6-BACKBONE_INTERFACE_STATE_DOWN L2-BM-6-ACTIVE_CLEAR L2-BM-6-ACTIVE_PROBLEM L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID L2-L2VPN_ICCP_SM-3-CONFIG_INVALID_NODEID_CLEAR
Satellite	PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_PROBLEM PKT_INFRA-ICPE_GCO-5-SATELLITE_STATUS_CLEAR

Type	Supported Events
Cluster	PLATFORM-REDDRV-7-ROLE_CHANGE PLATFORM-CE_SWITCH-6-UPDN PLATFORM-CLUSTER_CLM-6-UPDN LINK_UP LINK_DOWN
Celeborn cards	UEA_SPA_MODE-6-UEA_SPA_MODE_CHG
Configuration Commit syslogs	MGBL-CONFIG-6-DB_COMMIT SYS-5-CONFIG_I

However, in case of the following critical events, Cisco EPN Manager performs a full discovery of the device immediately when the event occurs:

SYS-5-RELOAD
SYS-5-RESTART
OIR-6-INSCARD
OIR-SP-6-INSCARD
SWT_CEFC_STATUS_CHANGE
cefcFRURemoved
cefcFRUInserted

Granular Inventory Event Flow Controllers

Granular inventory identifies the events generated and processes only the changes made in the devices. To avoid continuous syncing of devices due to event inflow, granular inventory uses Event Burst Flow Controller and Continuous Events Flow Controller.

Event Burst and Continuous Events are configurable only from the **/opt/CSCOlumos/conf/fault/correlationEngine/CE-EventBasedInventoryRules.xml** file.

Event Burst Flow Controller

When the number of incoming events for any technology for a managed device is greater than the threshold (BurstThreshold for BurstHoldOffTimer), Cisco EPN Manager considers it as an event burst condition. In this scenario, the granular inventory sync for the events breaching the threshold is held for a certain time period (BurstHoldOffTimer) until the event burst condition is cleared. This condition check is repeated at regular intervals. After the specified number of retries (BurstCheckRetryCount), if the threshold is still breached, Cisco EPN Manager stops all the granular inventory processing for the device.

If the event burst condition is detected and cleared before 3 retries, then the Event Burst Flow Controller triggers feature sync for the corresponding technology. If the event burst condition is detected and continues after 3 retries, then the controller stops all the granular inventory processing, raises the DISABLE_GRANULAR_INVENTORY_EVENT event, and disables the granular inventory for the device.

Table 58: Event Burst Action Properties

Property Name	Description	Default Value
BurstThreshold	The number of events of a given type over a period of time, which is considered as the 'burst' of that event type.	100 (events)
BurstHoldOffTimer	The time period for which the inventory sync is withheld.	300000 ms (5 mins)
BurstCheckRetryCount	The permitted number of retries.	3 (times)

After the granular inventory is disabled, a system check is initiated to monitor the event burst condition for the specific device; this system check will identify if the event burst condition continues. If there is no event burst condition, then it clears DISABLE_GRANULAR_INVENTORY_EVENT, followed by a full sync of the device. The granular inventory processing for the device will resume for any new incoming events.

Note When you enable the granular inventory for the device manually (see Enable or Disable Granular Inventory, on page 859), the corresponding DISABLE_GRANULAR_INVENTORY_EVENT is cleared.

Continuous Events Flow Controller

When the number of incoming events for a managed device is greater than the threshold (contEventsThresholdCount for contEventsCheckPeriod), Cisco EPN Manager considers it as continuous events condition. In this scenario, the granular inventory sync for the events breaching the threshold is held for a certain time period (contEventsDropPeriod) until the continuous events condition is cleared.

If the continuous events condition is detected, then the Continuous Events Flow Controller stops all the granular inventory processing for the device and raises the INVENTORY_SYNC_SUPPRESSED alarm to indicate that the device is in continuous state. It continues to perform feature sync at regular intervals, for all the events identified, until the continuous events condition is cleared.

Table 59: Continuous Event Action Properties

Property Name	Description	Default value
contEventsThresholdCount	Maximum number of allowed events at a time in the queue.	50 (events)
contEventsCheckPeriod	The time interval in milli-seconds, to check for the incoming event count.	300000 ms (5 mins)
contEventsDropPeriod	Time interval in milli-seconds, to trigger feature sync at regular intervals in case of continuous events.	300000 ms (5 mins)

Enable or Disable Granular Inventory

You can enable or disable granular inventory at the global level from the System Settings page. Choose **Administration** > **Settings** > **System Settings** > **Inventory** > **Inventory**, and then check or uncheck the **Enable Granular Inventory** check box. By default, this setting is enabled.

Note Disabling granular inventory will stop all the granular inventory processing for all the managed devices.

You can also enable or disable the granular inventory at the device level from the Network Devices page. To disable granular inventory for a device, select the required device in the Network Devices page, and then choose **Admin State** > **Disable Granular Inventory**. This will disable the granular inventory for the selected device only, and will not impact the granular inventory processing of any other devices in the system. To re-enable granular inventory for a device, select the required device in the Network Devices page, and then choose **Admin State** > **Enable Granular Inventory**. You can select one or more devices, and apply these actions. However, in case of multiple device selection, all the selected devices should be in either of the two states. If the selected devices are in mixed states, these options are not enabled.

Note If the granular inventory is disabled at the global level, then it precedes the granular inventory settings at the device level. If the granular inventory is enabled at the global level, then it succeeds the granular inventory settings at the device level.

Customize Generic Events That Are Displayed in the Web GUI

You can customize the description and severity for generic events generated by SNMP traps and syslogs. Your customization will be displayed in the Events tab for SNMP trap events. If a MIB module is not loaded, you can load it manually and then customize the notifications provided in that MIB.

See Customize Generic Events Based on SNMP Traps, on page 860, for information on how to customize these generic events.

Disable and Enable Generic Trap and Syslog Handling

By default Cisco Evolved Programmable Network Manager does not drop any received syslogs or traps. As mentioned in How are Alarms and Events Created and Updated?, on page 244, Cisco Evolved Programmable Network Manager maintains an event catalog that determines whether Cisco Evolved Programmable Network Manager should create a new event for incoming syslogs or traps (and if it creates a new event, whether it should also create an alarm). If Cisco Evolved Programmable Network Manager does not create an event, the trap or syslog is considered a *generic event* .

By default, Cisco Evolved Programmable Network Manager does the following:

- Displays the generic events in the Events list.
- Forwards generic events in e-mail or SNMP trap notifications, after normalizing them using CISCO-EPM-NOTIFICATION-MIB. For more information, refer to the CISCO-EPM-NOTIFICATION-MIB section in the guide.

All of these events are assigned the MINOR severity, regardless of the trap contents, and fall under the alarm category Generic.

Disable and Enable Generic Trap Processing

Use the genericTrap.sh command to manage generic syslogs.

To do the following:	Use this command:
Turn off generic trap processing	**/opt/CSCOlumos/bin/genericTrap.sh -l**
Turn on generic trap processing	**/opt/CSCOlumos/bin/genericTrap.sh -u**

Customize Generic Events Based on SNMP Traps

Cisco EPN Manager supports the customized representation of generic events in the GUI. Managed objects normally generate SNMP traps and notifications that contain an SNMP trap object identifier (SnmpTrapOID) and a variable bind object identifier (VarBindOIDs) in numerical format. Cisco EPN Manager translates the numeric SnmpTrapOIDs and VarBindOIDs into meaningful names using customized MIB modules, then displays the generic events in the web GUI (in the event tables, Device 360 view, and so forth). For more details on Generic Events see How are Alarms and Events Created and Updated?, on page 244.

Using the SNMP MIB files that are packaged with Cisco EPN Manager, you can customize the defined MIBs for your deployment's technology requirement.

The following table illustrates how ObjectIDs are decoded and displayed in the GUI.

Table 60: Example: ObjectID Representation

OIDs before Decoding	OIDs after Decoding
`snmpTrapOID = 1.3.6.1.4.1.9.10.120.0.1', Values: 1.3.6.1.4.1.9.10.119.1.1.2.1.11.7.1=1`	`mplsL3VpnVrfDown, values: mplsL3VpnVrfOperStatus.("vrf1").(1) = 1`

Follow the steps below to create customized generic events.

Step 1 Select **Monitor** > **Monitoring Tools** > **Alarms and Events**.

Step 2 Click the **Events** tab.

Step 3 Click **Custom Trap Events** and then click **Add**.

Step 4 In the **Add New Custom Trap Events** window,upload a MIB file and enter the required details.

Step 5 If you upload a new MIB file, wait until the file upload is complete, and then click **Refresh MIBs** to have the newly added MIB included in the **MIB** drop-down list.

Step 6 Click **OK**.

Cisco EPN Manager creates a new event type and alarm condition for the specified trap.

Troubleshoot Fault Processing Errors

If your deployment has fault processing problems, follow this procedure to check the fault logs.

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

Step 2 Select **Administration** > **Settings** > **Logging**, then choose the **Global Settings** tab.

Step 3 Click **Download** to download all the server log files.

Step 4 Compare the activity recorded in these log files with the activity you are seeing in your management application:

console.log

ncs-x-x.log

decap.core.java.log

xmp_correlation.log

decap.processor.log

Note You will not be able to reset the Global Settings by clicking **Reset** from Cisco EPN Manager.

What to do next

You can also get help from the Cisco support community. If you do need to open a support case, attach the suspect log files with your case. See Get Help from the Cisco Support Community and Technical Assistance Center (TAC), on page 861.

Get Help from the Cisco Support Community and Technical Assistance Center (TAC)

Open a Cisco Support Case

When you open a support case from the web GUI, Cisco EPN Manager automatically populates the case form with information it can retrieve from a device. This includes technical details about the device, configuration changes on the device, and all device events that occurred in the last 24 hours. You can also attach your own files to the case.

Before you begin

You can open a support case from the web GUI if:

- Your administrator has configured Cisco EPN Manager to allow you to do so. See Set Up Defaults for Cisco Support Requests, on page 778.

- The Cisco EPN Manager server has a direct connection to the internet, or a connection by way of a proxy server.
- You have a Cisco.com username and password.

Step 1 Choose one of the following:

- From **Monitor** > **Monitoring Tools** > **Alarms and Events**. Select a single alarm, click the >> icon and then choose **Troubleshoot** > **Support Case**. If you do not see the **Troubleshoot** button, widen your browser window.
- From the Device 360 view. Hover your mouse over a device IP address, then click the information icon. Choose **Support Request** from the **Actions** drop-down menu.

Step 2 Enter your Cisco.com username and password.

Step 3 Click **Create**. Cisco EPN Manager populates the form with data it retrieves from the device.

Step 4 (Optional) Enter a Tracking Number that corresponds to your own organization's trouble ticket system.

Step 5 Click **Next** and enter a description of the problem.

Cisco EPN Manager populates the form with data it retrieves from the device and automatically generates the necessary supporting documents.

If desired, upload files from your local machine.

Step 6 Click **Create Service Request**.

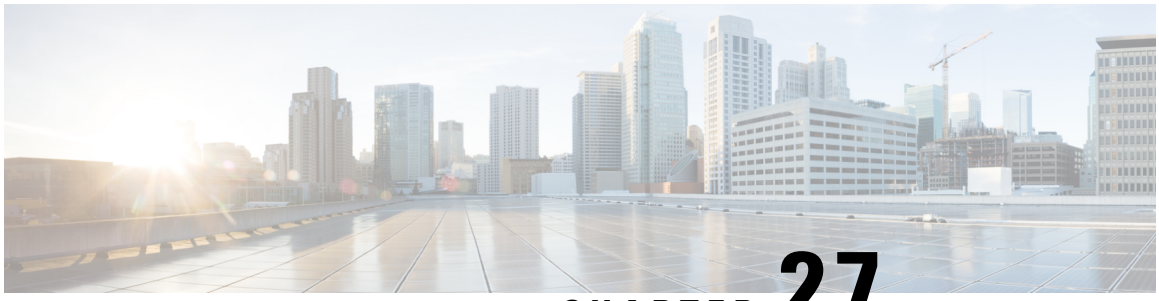
Join the Cisco Support Community

You can access and participate in discussion forums in the online Cisco Support Community. You will need a Cisco.com username and password.

Step 1 Choose one of the following:

- From **Monitor > Monitoring Tools > Alarms and Events**. Click a single alarm, then choose **Troubleshoot > Support Forum**. If you do not see the **Troubleshoot** button, widen your browser window.
- From the Device 360 view. Hover your mouse over a device IP address, then click the information icon. Choose **Support Community** from the **Actions** drop-down menu.

Step 2 In the Cisco Support Community Forum page, enter your search parameters to find what you need.



CHAPTER 27

Audits and Logs

Audit Changes Made By Users (Change Audit)

Cisco EPN Manager supports managing change audit data in the following ways:

Enable Change Audit Notifications and Configure Syslog Receivers

If desired, you can configure Cisco EPN Manager to send a change audit notification when changes are made to the system. These changes include device inventory and configuration changes, configuration template and monitoring template operations, and user operations such as logins and logouts and user account changes.

You can configureCisco EPN Manager to:

- Forward changes as change audit notifications to a Java Message Server (JMS).
- Send these messages to specific syslog receivers.

If you configure syslog receivers but do not receive syslogs, you may need to change the anti-virus or firewall settings on the destination syslog receiver to permit reception of syslog messages.

Step 1 Select **Administration** > **Settings** > **System Settings**, then choose **Mail and Notification** > **Change Audit Notification**.

Step 2 Select the **Enable Change Audit Notification** check box to enable notifications.

Step 3 If you want to send the messages to specific syslog receivers:

a) Click the **Add** button (+) to specify a syslog receiver.

b) In the **Syslog Receivers** area, enter the IP address, protocol , and port number of the syslog receiver.

You can repeat these steps as needed to specify additional syslog receivers.

Step 4 Click **Save**.

Note It is recommended to restart the Cisco EPN Manager server for the records to be reflected in secure tls log.

View Change Audit Details

Step 1 Log in to Cisco EPN Manager as an administrator.

Step 2 Choose **Monitor** > **Tools** > **Change Audit Dashboard**.

The **Change Audit Dashboard** displays audit data:

- Device management
- User management
- Configuration template management
- Device community and credential changes
- Inventory changes of devices
- Service discovery
- Alarms, RESTConf
- Job management assurance

The **Change Audit report** and **Change Audit** dashboard display the details irrespective of the virtual domain you are logged in.

The **Change Audit Dashboard** screen also displays the Device Name apart from other details such as IP Address, Audit Description, User Name, Audit Name, and Client IP Address. Click the *i* icon next to the IP Address field to view the Device 360 details.

Note If you have logged in as a root user, then you can view all the Audit changes. If you have logged in as a non-root user, then you can only view the Audit changes performed by you.

Forward OS Logs to Remote System

To enable EPNM to forward OS CLI system logs to a remote system or to configure the log level, use the following logging command in configuration mode.

Note You can configure only one remote system to forward the logs to.

logging {ip-address | hostname} {loglevel level}

Where,

Syntax	Description
ip-address	IP address of remote system to which you forward the logs to. Up to 32 alphanumeric characters.
hostname	Hostname of remote system to which you forward the logs to. Up to 32 alphanumeric characters.
loglevel	The command to configure the log level for the logging command.
level	Number of the desired priority level at which you set the log messages. Priority levels are (enter the number for the keyword): • 0 - emerg—Emergencies: System unusable • 1 - alert—Alerts: Immediate action needed • 2 - crit—Critical: Critical conditions • 3 - err—Error: Error conditions • 4 - warn—Warning: Warning conditions • 5 - notif—Notifications: Normal but significant conditions • 6 - inform—(Default) Informational messages • 7 - debug—Debugging messages

To disable this function, use the no form of this command.

This command requires an **IP address** or **hostname** or the **loglevel** keyword. An error occurs if you enter two or more of these arguments.

Example 1:

```
ncs/admin(config)# logging 209.165.200.225
ncs/admin(config)#
```

Example 2:

```
ncs/admin(config)# logging loglevel 0
ncs/admin(config)#
```

System Logs

Cisco EPN Manager provides two classes of logs which are controlled by choosing **Administration** > **Settings** > **Logging**.

Logging Type	Description	See:
General	Captures information about actions in the system.	View and Manage General System Logs, on page 866
Syslog	Forwards Cisco EPN Manager audit logs (as syslogs) to another recipient.	Forward System Audit Logs As Syslogs, on page 867

View and Manage General System Logs

You can view system logs after downloading them to your local server.

View the Logs for a Specific Job

Step 1 Choose **Administration** > **Dashboards** > **Job Dashboard** .

Step 2 Choose a job type from the Jobs pane, then click on a job instance link from the Jobs window.

Step 3 At the top left of the Job instance window, locate **Log file**, then click **Download**.

Note You can download the logs only for Configuration Archive Software, Configuration Rollback, Configuration Overwrite, and Configuration Deploy job types.

Step 4 Open or save the file as needed.

Adjust General Log File Settings and Default Sizes

By default, Cisco EPN Manager logs all error, informational, and trace messages generated by all managed devices.

It also logs all SNMP messages and Syslogs that it receives.

You can adjust these settings, changing logging levels for debugging purposes.

To do the following:	From Administration > Settings > Logging:
Change the size of logs, number of logs saved, and the file compression options	Adjust the Log File Settings. **Note** Change these settings with caution to avoid impacting the system. As per log4j MaxBackupIndex, there will be one main file accompanied by the set number of backup files. For example, if the number of log files is set to 3, there is one main file (.log) and 3 backup files (.log.1, .log.2, and .log.3). If the **Number of files** is modified to a value lower than the one previously set, the log file settings are applied only to the newly generated files. For example, if the preset value was 5 and now you modify it to 2, the settings will only be applied to files .log, .log.1 and .log.2. There is no changes to the files .log.3, .log.4, and .log.5. If you select the **Compression (Zip)** option, log files are compressed and archived in the `./logs/backup/[logging_module]` folder of the process. Retention of the compressed log files is subject to the criteria: • Storage (MB): Maximum size of the folder in MB • Number of Days: Maximum age of the log files The purge is triggered when either of the criteria is met. Optionally, if **Backup to external location** is enabled, log files marked for cleanup are copied to the specified external repository prior to deletion.
Change the logging level for specific modules	In the General Log Settings, select the files and the desired level, and click **Save**. For example, from the **Message Level** drop-down list, choose one of the following as current logging level: • Error—Captures error logs on the system. • Information—Captures informational logs on the system. • Trace—Reproduces problems of managed devices on the system so the details can be captured in the logs. • Debug—Captures debugging logs on the system. When you restart Cisco EPN Manager , the log level resets to Error.
Download log files for troubleshooting purposes	In the **Global Settings** tab, click **Download**.

Forward System Audit Logs As Syslogs

Before you begin

To work with Forward System Audit Logs as Syslogs, the user must configure Enable Change Audit Notifications and Configure Syslog Receivers.

Step 1 Choose **Administration** > **Settings** > **Logging**, then choose **Syslog** tab to view **Syslog Settings**.

Step 2 Select the **Enable Syslog** check box to enable collecting and processing system logs.

Step 3 In the **Syslog Host** field, enter the IP address of the destination server.

Step 4 From the **Syslog Facility** drop-down list, choose any local use facilities for sending syslog messages. The local use facilities are not reserved and are available for general use.

Step 5 Click **Save**.

Note If you enable system logs forwarding to remote server through an admin CLI, logs will not be registered to ade.log file.

Audit Log

Cisco EPN Manager logs the information displayed under **Monitor** > **Tools** > **Change Audit Dashboard** in the `audit.log`. Logging is enabled by default. This information is logged irrespective of message level or log module changes.

If you want to export the audit logs in a CSV format, click the **Export** icon to export the data. Enter the details to extract the logs and click **Export**. If you want to export the data for only few records, select the required rows or use the **Filter** option and click **Export**. Only selected data is exported.

Device-Specific Logging

Cisco EPN Manager enables you to store the XDE and Inventory logs in DEBUG mode for specific devices. You can enable or disable the logging from SSH CLI. (See Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Enable device-specific logging

Important Before you enable device-specific logging for XDE or inventory logs, ensure that you have set the global log level to INFO by running the following command:

`/opt/CSCOlumos/bin/setLogLevel.sh` *`logName`* `INFO`

logName - Enter xde or inventory as necessary.

To enable device-specific logging, run the following command:

`/opt/CSCOlumos/bin/setDeviceLevelDebug.sh` *`logName`* `DEBUG` *`deviceIP`*

Where:

- *logName* - Enter xde or inventory as necessary. Enabling device-specific logging for inventory logs enables logging for ifm_inventory logs as well.

- *deviceIP* - Specify the IP address of the device for which you want to enable the logging. You may specify multiple IP addresses in the same command separated by a comma.

The inventory or XDE logs in DEBUG mode are stored only for the specified device(s). For other devices, only INFO logs are stored. The log files generated during sync are *xde.log.**, *inventory.log.** and *ifm_inventory.log.**.

Cisco EPN Manager overrides previously specified IP address with the IP address that you specify each time you run this command.

Example

For Inventory logs:

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh inventory DEBUG 1.2.3.4,5.6.7.8
```

For XDE logs:

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh xde DEBUG 1.2.3.4,5.6.7.8
```

View list of devices for which device-specific logging is enabled

To view the list of devices for which device-specifc logging is enabled, run the following command:

```
/opt/CSCOlumos/bin/listDeviceLevelDebug.sh logName
```

logName - Enter xde or inventory as necessary.

Example

```
/opt/CSCOlumos/bin/listDeviceLevelDebug.sh inventory
```

Disable device-specific logging

To disable device-specific logging for the specified log, set the log level to INFO. This disables device-specific logging for all devices

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh logName INFO
```

logName - Enter xde or inventory as necessary.

Note You cannot disable logging for specific devices.

Example

```
/opt/CSCOlumos/bin/setDeviceLevelDebug.sh inventory INFO
```

Inventory Discovery Process Logs

The logs for inventory-discovery-process are available at:
`/opt/CSCOlumos/logs/inventory-discovery-process`

To change log level for inventory-discovery-process, enter the following commands in the admin CLI (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765):

- To change the log level to INFO:

```
/opt/CSCOlumos/bin/setLogLevel.sh logName INFO inventory-discovery-process
```

- To change the log level to DEBUG:

```
/opt/CSCOlumos/bin/setLogLevel.sh logName DEBUG inventory-discovery-process
```

logName- Enter XDE or Inventory as necessary.

Synchronize System Logs to an External Location

You can configure to synchronize the *ncs* (Cisco EPN Manger logs) and *os* logs to a local or NFS based repository.

To synchronize the logs to a repository:

Before you begin

Create a local or NFS based repository to which you want to synchronize the logs. For more information on how to do this, see Set Up and Manage Repositories, on page 736.

Step 1 Open a CLI session with the Cisco EPN Manager server. See Connect via CLI, on page 752.

Step 2 Enter the following commands in the configuration mode to synchronize the system logs.

- To synchronize the *ncs* logs:

```
logging sync-logs ncs repository repository-name
```

- To synchronize the *os* logs:

```
logging sync-logs os repository repository-name
```

Where *repository-name* refers to the repository you configured.

Note To disable the synchronization, enter these commands instead in the configure terminal mode.

- To disable synchronizing the *ncs* logs:

```
no logging sync-logs ncs repository repository-name
```

- To disable synchronizing the *os* logs:

```
no logging sync-logs os repository repository-name
```

Step 3 Exit configuration mode:

```
exit
```

Example

Example 1

```
(config)# logging sync-logs ncs repository myrepository
(config)# logging sync-logs os repository myrepository
config# exit
```

Example 2

```
(config)# no logging sync-logs ncs repository myrepository
(config)# no logging sync-logs os repository myrepository
config# exit
```

Security Log

Cisco EPN Manager maintains a log of security-related actions performed by a root user and members of the admin and super-user user group in active and past web GUI or CLI sessions.

The logged information includes a description of the event, the IP address of the client from which the user performed the task, and the time at which the task was performed. The following events are logged:

- User login
- User logout
- User creation
- User added
- User deleted
- Lock user
- Unlock user
- Linux shell entering
- User modifications (mail, password)

To view details of this log, enter the following command. You must be logged in as an admin CLI user to use this command. For more information, see Establish an SSH Session With the Cisco EPN Manager Server, on page 765.

```
show logging security
```

Cisco EPN Manager always maintains a log of security-related actions locally.

Event entries from the CLI have the prefix “SYSTEM-CLI:” and entries from the web interface have the prefix “SYSTEM-WEB:” The structure of each event entry is based on a JSON format and is JSON valid.

Events CLI	• SYSTEM-CLI:SSH:LOGIN:FAILED:WRONG_PASSWORD • SYSTEM-CLI:SSH:LOGIN:FAILED:MAXIMUM_ATTEMPTS_REACHED • SYSTEM-CLI:SSH:LOGIN:SUCCESSFUL

	• SYSTEM-CLI:SSH:LOGOUT:SUCCESSFUL • SYSTEM-CLI:CONSOLE:LOGIN:WRONG_PASSWORD • SYSTEM-CLI:CONSOLE:LOGIN:SUCCESSFUL • SYSTEM-CLI:CONSOLE:LOGOUT:SUCCESSFUL • SYSTEM-CLI:USER:ADD • SYSTEM-CLI:USER:DELETE • SYSTEM-CLI:USER:GROUP • SYSTEM-CLI:USER:PASSWORD • SYSTEM-CLI:USER:PASSWORD:POLICY • SYSTEM-CLI:USER:ROLE • SYSTEM-CLI:USER:STATE:LOCK • SYSTEM-CLI:USER:STATE:UNLOCK • SYSTEM-CLI:USER:MAIL • SYSTEM-CLI:USER:OS:SHELL:ENTERED • SYSTEM-CLI:OS:SHELL:ENABLED • SYSTEM-CLI:OS:SHELL:DISABLED
Events UI	• SYSTEM-WEB:UI:NCS:BODGE:LOGIN:SUCCESSFUL • SYSTEM-WEB:UI:LOGOUT • SYSTEM-WEB:UI:LOGIN:SUCCESSFUL • SYSTEM-WEB:UI:LOGIN:AUTHENTICATION_FAILED • SYSTEM-WEB:UI:USER:DELETE • SYSTEM-WEB:UI:USER:ADD • SYSTEM-WEB:UI:USER:STATE:UNLOCK • SYSTEM-WEB:UI:USER:STATE:LOCK • SYSTEM-WEB:UI:USER:UPDATE • SYSTEM-WEB:HM:LOGIN:AUTHENTICATION_FAILED

Send Security Log to an External location

Remote logging is supported and you can configure to forward security-related events to a remote syslog server.

Step 1 Open a CLI session with the Cisco EPN Manager server, making sure you enter configure terminal mode. See Connect via CLI, on page 752.

Step 2 Enter the following command:

```
logging security hostname[:port]
```

Where *hostname* is the name or IP address of the remote logging host server.

Note This command sends the log to UDP port 514 by default, if the port is not specified.

Step 3 Exit the configuration mode:

```
exit
```

Example

```
/admin(config)# logging security a.b.c.d
/admin(config)# exit
```

Security Events Log

Cisco EPN Manager maintains a log of the following events in the security_events.log files.

- Sessions created or destroyed over cryptographics protocols
- Probable security attacks

Events related to security attacks are logged by default. You must enable logging of cryptographic sessions-related information by setting the log level to **Info**. To do this, run the following command in admin CLI at /opt/CSCOlumos/bin in the server path.

```
./setLogLevel.sh SecurityEvents.crypto INFO
```

Event type	Events	Information Logged
Events related to security attacks	SQL and LDAP injections	Input validation errors, irrespective of the source of the data. The logged data includes the reason why the data is invalid.
Information related to cryptographic sessions	Sessions created and destroyed over the following protocols: • raw • SSH2, Telnet • NETCONF • TL1	• Notification type • Target device • Connection port • Username • Connection type • Session details

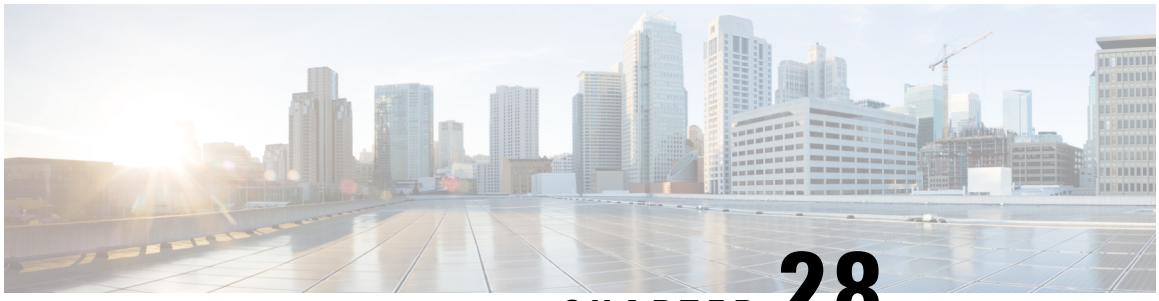
You can view the content of the log by entering the following commands in the admin CLI. See Establish an SSH Session With the Cisco EPN Manager Server, on page 765 for more information.

```
less /opt/CSCOlumos/logs/security_events.log
```

```
less /opt/CSCOlumos/logs/security_events.log.x
```

Where:

- *x* is a number greater than or equal to 1 since this is a rolling event log file.



CHAPTER 28

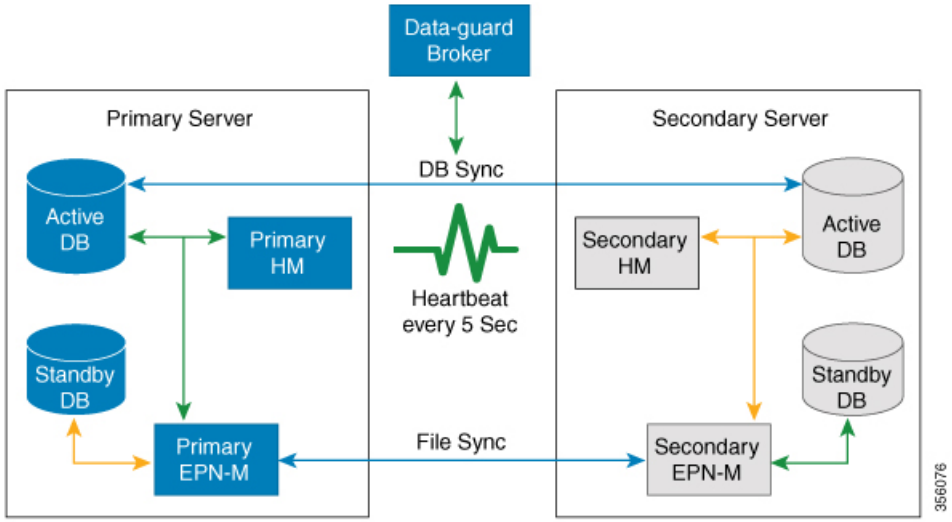
Configure and Manage High Availability

How High Availability Works

The Cisco EPN Manager high availability (HA) framework 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. Servers can fail due to issues in one or more of the following areas:

- Application processes—Server, TFTP, FTP, and other process failures. You can view the status of these processes using the CLI **ncs status** command.
- Database server—Database-related process failures (the database server runs as a service on Cisco EPN Manager).
- Network—Problems with network access or reachability.
- System—Problems with the server's physical hardware or operating system.
- Virtual machine (if HA is running in a VM environment)—Problems with the VM environment on which the primary and secondary servers are installed.

The following figure shows the main components and process flows for an HA setup.



An HA deployment consists of a primary and a secondary server with Health Monitor (HM) instances (running as an application process) on both servers. When the primary server fails (either automatically 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 failover. This HA is based on the *active/passive* or *cold standby* model of operation. Because it is not a clustered system, when the primary server fails, the sessions are not preserved in the secondary server.

When issues on the primary server are resolved and the server is in a running state, it remains in standby mode during which it begins syncing its data with the active secondary server. When the primary is available again, you can initiate a failback operation. When a failback is triggered, the primary server again takes over the active role. This role switching between the primary and secondary servers happens within two to three minutes.

Whenever the HA configuration determines that the primary server has changed, it synchronizes this change with the secondary server. These changes are of two types:

- File changes, which are synchronized using the HTTPS protocol. This includes items such as report configurations, configuration templates, TFTP-root directory, administration settings, licensing files, and the key store. File synchronization is done:
  - In batches, for files that are not updated frequently (such as license files). These files are synchronized once every 500 seconds.
  - Near real-time, for files that are updated frequently. These files are synchronized once every 11 seconds.
- Database changes, such as updates related to configuration, performance and monitoring data. Oracle Recovery Manager (RMAN) creates the initial standby database and Oracle Active Data Guard synchronizes the databases when there is any change.

The primary and secondary HA servers exchange the following messages to maintain synchronization between the two servers:

- Database Sync—Includes all the information necessary to ensure that the databases on the primary and secondary servers are running and synchronized.

- File Sync—Includes frequently updated configuration files. These are synchronized every 11 seconds, while other infrequently updated configuration files are synchronized every 500 seconds.

Note Configuration files that are updated manually on the primary are not synced to the secondary. When you update a configuration file manually on the primary, you must update the file on the secondary as well.

- Process Sync—Ensures that application- and database-related processes are running. These messages fall under the Heartbeat category.
- Health Monitor Sync—These messages check for the network, system, and health monitor failure conditions.

About Primary and Secondary Servers

In any EPN Manager high availability (HA) implementation, for a given instance of a primary server, there must be only one dedicated secondary server.

Typically, each HA server has its own IP address or host name. If you place the servers on the same subnet, they can share the same IP using virtual IP addressing, which simplifies device configuration.

To configure a HA deployment, you can use either a network interface eth0 or a NIC teaming interface. If you use NIC teaming interface for HA deployment, then you must designate it as "Northbound Interface". For more information, see NIC Teaming with HA, on page 886

Note Configuring virtual IP on the NIC teaming interface may work. However, this type of configuration is not officially certified.

Once HA is set up, you must avoid changing the IP addresses or host names of the HA servers. This breaks the HA setup.

For more information, see Reset the Server IP Address or Host Name, on page 913.

Note

- For HA configured servers, the EPNM title bar displays the type of server you are connected to, that is, whether you are connected to a primary server or secondary server.
- If the primary server is active and the secondary server is down for a period that is longer than the configured retention time, the HA configuration will be removed. By default, the configured retention time is 6 hours.

Planning HA Deployments

The HA feature supports the following deployment models:

- **Local**: Both of the HA servers are located on the same subnet (giving them Layer 2 proximity), usually in the same data center.
- **Campus**: Both HA servers are located in different subnets connected via LAN. Typically, they will be deployed on a single campus, but at different locations within the campus.
- **Remote**: Each HA server is located in a separate, remote subnet connected via WAN. Each server is in a different facility. The facilities are geographically dispersed across countries or continents.

The following sections explain the advantages and disadvantage of each model, and discusses underlying restrictions that affect all deployment models.

HA will function using any of the supported deployment models. The main restriction is on HA's performance and reliability, which depends on the bandwidth and latency criteria discussed in "Network Throughput Restrictions on HA". As long as you are able to successfully manage these parameters, it is a business decision (based on business parameters, such as cost, enterprise size, geography, compliance standards, and so on) as to which of the available deployment models you choose to implement.

Network Throughput Restrictions on HA

Cisco EPN Manager HA performance is always subject to the following limiting factors:

- The net bandwidth available to Cisco EPN Manager for handling all operations. These operations include (but are not restricted to) HA registration, database and file synchronization, and triggering failback.
- The net latency of the network across the links between the primary and secondary servers. Irrespective of the physical proximity of these two servers, high latency on these links can affect how the Cisco EPN Manager maintains sessions between the primary and secondary servers.
- The net throughput that can be delivered by the network that connects the primary and secondary servers. Net throughput varies with the net bandwidth and latency, and can be considered a function of these two factors.

These limits apply to at least some degree in every possible deployment model, although some models are more prone to problems than others. For example: Because of the high level of geographic dispersal, the Remote deployment model is more likely to have problems with both bandwidth and latency. But both the Local and Campus models, if not properly configured, are also highly susceptible to problems with throughput, as they can be saddled by low bandwidth and high latency on networks with high usage.

You rarely see throughput problems affecting a failback or failover, as the two HA servers are in more or less constant communication and the database changes are replicated quickly. Most failovers and failbacks take approximately two to three minutes.

The main exception to this rule is the delay for a full database copy operation. This kind of operation is triggered when the primary server has been down for more than the data retention period and you then bring it back up. The data retention period for the express, express-plus, and standard configurations server is six hours and for professional and Gen 2 appliance server it is 12 hours.

Cisco EPN Manager triggers a full database copy operation from the secondary to the primary. No failback is possible during this period, although the Health Monitor page displays any events encountered while the database copy is going on. When the copy is complete, the primary server goes to the "Primary Synching" state, and you can then trigger failback. Be sure not to restart the primary server or disconnect it from the network while the full database copy is in progress.

Variations in net throughput during a full database copy operation, irrespective of database size or other factors, can mean the difference between a database copy operation that completes successfully in under an hour and one that does not complete at all. Cisco has tested the impact of net throughput on HA deployment in configurations following the Remote model, using typical Cisco EPN Manager database sizes of 105–156 GB. Based on these tests, Cisco recommends for a typical database of 125 GB (generating a 10 GB backup file):

- For best results: With sub-millisecond latency, and net throughput of 977 Mbps or more, expect a complete database copy time of one hour or less.
- For good results: With latency of 70 milliseconds, and net throughput of 255 Mbps or more, expect a complete database copy time of two hours or less.
- For acceptable results: With latency of 220 milliseconds or less, and net throughput of 86 Mbps or more, expect a complete database copy time of 4.5 hours or less.

With latencies of 330 ms or higher, and throughput of 46 Mbps or less, you run the risk of the database copy not completing successfully.

Related Topics

Planning HA Deployments, on page 877
Using the Remote Model, on page 880

Using the Local Model

The main advantage of the Local deployment model is that it permits use of a virtual IP address as the single management address for the system. Users can use this virtual IP to connect to Cisco EPN Manager, and devices can use it as the destination for their SNMP trap and other notifications.

The only restriction on assigning a virtual IP address is to have that IP address in the same subnet as the IP address assignment for the primary and secondary servers. For example: If the primary and secondary servers have the following IP address assignments within the given subnet, the virtual IP address for both servers can be assigned as follows:

- Subnet mask: 255.255.255.224 (/27)
- Primary server IP address: 10.10.101.2
- Secondary server IP address: 10.10.101.3
- Virtual IP address: 10.10.101.[4-30] e.g., 10.10.101.4. Note that the virtual IP address can be any of a range of addresses that are valid and unused for the given subnet mask.

In addition to this main advantage, the Local model also has the following advantages:

- Usually provides the highest bandwidth and lowest latency.
- Simplified administration.
- Device configuration for forwarding syslogs and SNMP notifications is much easier.

The Local model has the following disadvantages:

- Being co-located in the same data center exposes them to site-wide failures, including power outages and natural disasters.

- Increased exposure to catastrophic site impacts will complicate business continuity planning and may increase disaster-recovery insurance costs.

Using the Campus Model

The Campus model assumes that the deploying organization is located at one or more geographical sites within a city, state or province, so that it has more than one location forming a "campus". This model has the following advantages:

- Usually provides bandwidth and latency comparable to the Local model, and better than the Remote model.
- Is simpler to administer than the Remote model.

The Campus model has the following disadvantages:

- More complicated to administer than the Local model.
- Does not permit use of a virtual IP address as the single management address for the system, so it requires more device configuration (see "What If I Cannot Use Virtual IP Addressing?" in Related Topics).
- May provide lower bandwidth and higher latency than the Local model. This can affect HA reliability and may require administrative intervention to remedy (see "Network Throughput Restrictions on HA" in Related Topics).
- While not located at the same site, it will still be exposed to city, state, or province-wide disasters. This may complicate business continuity planning and increase disaster-recovery costs.

Related Topics

Planning HA Deployments, on page 877
Network Throughput Restrictions on HA, on page 878
Using the Local Model, on page 879
Using the Remote Model, on page 880
What If I Cannot Use Virtual IP Addressing?, on page 884

Using the Remote Model

The Remote model assumes that the deploying organization has more than one site or campus, and that these locations communicate across geographical boundaries by WAN links. It has the following advantages:

- Least likely to be affected by natural disasters. This is usually the least complex and costly model with respect to business continuity and disaster recovery.
- May reduce business insurance costs.

The Remote model has the following disadvantages:

- More complicated to administer than the Local or Campus models.
- Does not permit use of a virtual IP address as the single management address for the system, so it requires more device configuration (see "What If I Cannot Use Virtual IP Addressing?" in Related Topics).

- Usually provides lower bandwidth and higher latency than the other two models. This can affect HA reliability and may require administrative intervention to remedy (see “Network Throughput Restrictions on HA” in Related Topics).

Related Topics

Planning HA Deployments
Network Throughput Restrictions on HA, on page 878
Using the Local Model
Using the Campus Model, on page 880
What If I Cannot Use Virtual IP Addressing?, on page 884

Automatic Versus Manual Failover

Configuring HA for automatic failover reduces the need for network administrators to manage HA. It also reduces the time taken to respond to the conditions that provoked the failover, since it brings up the secondary server automatically.

However, we recommend that the system be configured for Manual failover under most conditions. Following this recommendation ensures that the Cisco EPN Manager does not go into a state where it keeps failing over to the secondary server due to intermittent network outages. This scenario is most likely when deploying HA using the Remote model. This model is often especially susceptible to extreme variations in bandwidth and latency.

If the failover type is set to Automatic and the network connection goes down or the network link between the primary and secondary servers becomes unreachable, there is also a small possibility that the primary and secondary servers activate at the same time. We refer to this as the “split brain scenario”.

To prevent this, the primary server always checks to see if the secondary server is Active. When the network connection or link is restored and the primary is able to reach the secondary again, the primary server checks the secondary server's state. If the secondary state is Active, then the primary server goes down on its own. Users can then trigger a normal, manual failback to the primary server.

This scenario *only* occurs when the primary HA server is configured for Automatic failover. Configuring the primary server for Manual failover eliminates the possibility of this scenario. This is another reason why we recommend Manual failover configuration.

Automatic failover is especially ill-advised for larger enterprises. If a particular HA deployment chooses to go with Automatic failover anyway, an administrator may be forced to choose between the data that was newly added to the primary or to the secondary. This means, essentially, that there is a possibility of data loss whenever a split-brain scenario occurs. To tackle this issue, see “How to Recover From Split-Brain Scenario” in Related Topics.

To ensure that HA is managed correctly, Cisco recommends that the Cisco EPN Manager administrators always confirm the overall health of the HA deployment before initiating failover or failback, including:

- The current state of the primary.
- The current state of the secondary.
- The current state of connectivity between the two servers.

Related Topics

Planning HA Deployments, on page 877
Network Throughput Restrictions on HA, on page 878

Trigger Failback, on page 896
How to Recover From Split-Brain Scenario, on page 906
Enable HA for Operations Center

Set Up High Availability

The Cisco Evolved Programmable Network Manager Installation Guide describes how to install the primary and secondary servers in your high availability deployment. As part of the installation, your administrator configures your HA deployment to use manual or automatic failover. You can check the current failover setting using the **ncs ha status** command or by checking the Health Monitor web page (see Use the Health Monitor Web Page, on page 893).

After the primary and secondary servers are installed, you must perform the HA configuration steps described in How to Configure HA Between the Primary and Secondary Servers, on page 884.

The following topics provide additional information about the HA deployment:

- Using Virtual IP Addressing With HA, on page 882
- What If I Cannot Use Virtual IP Addressing?, on page 884
- How to Configure HA Between the Primary and Secondary Servers, on page 884
- Configure an SSO Server in an HA Environment, on page 887

Using Virtual IP Addressing With HA

A virtual IP address represents the management IP address of the active HA server. During failover or failback, the virtual IP address automatically switches between the two HA servers. This provides two benefits:

- You do not need to know which server is active in order to connect to the Cisco EPN Manager web GUI. Using a virtual IP, your requests are automatically forwarded to the HA server that is active.
- You do not need to configure managed devices to forward notifications to both the primary server and the secondary server. Notifications only need to be forwarded to the virtual IP address.

Virtual IP addressing can be enabled when you configure the secondary server with the primary server. You will need to provide the virtual address (IPv4 is mandatory while IPv6 is optional) that you want both servers to share. See How to Configure HA Between the Primary and Secondary Servers, on page 884.

Using virtual IP addresses does not change the fact that active client-server sessions are terminated when a failover or failback occurs. Even though the virtual IP address will remain available, active client-server sessions (web GUI or NBI) are terminated as the new server begins servicing new requests. Web GUI users will have to log out and back in. For information on handling broken NBI sessions, see the Cisco Evolved Programmable Network Manager MTOSI API Guide for OSS Integration.

Note To use a virtual IP, the IP addresses of the primary and secondary servers must be on the same subnet.

Multiple Virtual IP Addressing with HA

With Cisco EPN Manager, you can configure up to three interfaces to have their own virtual IP address. In addition, a team (logical binding) of multiple interfaces can be configured with a virtual IP address. There are two ways to do this.

- (**recommended**) Configure all virtual IP addresses from CLI.

  In this case, do not select the **Enable Virtual IP** check box in Cisco EPN Manager UI. This field check box is automatically populated with the first virtual IP address that you configure from CLI.

- Configure the first virtual IP address from the Cisco EPN Manager UI and configure the remaining virtual IP addresses from CLI.

Note To avoid issues during HA registration, ensure that the first virtual IP you configure from CLI matches with what you have configured in UI. In case there is a mismatch, HA registration is blocked and an error message is displayed.

This process is a prerequisite for performing HA registration.

To enable multiple virtual IPs from CLI:

Step 1 Log into the server as the Cisco EPN Manager CLI admin user.

Step 2 Enter configuration mode.

```
configure terminal
```

Step 3 Choose the interface on which you would like to configure the virtual IP.

```
interface <name of interface>
```

Step 4 Enter the following command at the prompt.

```
virtual-ip
```

Step 5 Specify the IPv4 virtual IP address that is to be shared by the primary and secondary HA servers. Optionally, specify an IPv6 virtual IP address (An IPv4 address is mandatory while IPv6 address is optional).

- (mandatory) To configure an IPv4 address:

  ```
  ip-address IPv4 address
  ```

- (optional) To configure an IPv6 address:

  ```
  ipv6-address IPv6 address
  ```

Step 6 Exit the sub-menu.

```
exit
```

Step 7 Exit the interface configuration

```
exit
```

Step 8 Exit the configuration mode.

```
exit
```

Step 9 (Optional) Verify the configuration by running the following command on the interface

```
show running-config
```

The virtual IP addresses are enabled on the primary server once HA registration has completed successfully. The virtual IP addresses are copied to the secondary server during HA registration, but are enabled only in case of a failover.

Note

- The Cisco EPN Manager UI displays the virtual IP configured on the first interface – GigabitEthernet 0 (or Ethernet 0) only. Virtual IP addresses configured on remaining interfaces are not displayed in the web UI.
- To view all virtual IP addresses configured on an interface, run the `show running config` command in CLI.

What If I Cannot Use Virtual IP Addressing?

Depending on the deployment model you choose, not configuring a virtual IP address may result in the administrator having to perform additional steps in order to ensure that syslogs and SNMP notifications are forwarded to the secondary server in case of a failover. The usual method is to configure the devices to forward all syslogs and traps to both servers, usually via forwarding them to a given subnet or range of IP addresses that includes both the primary and secondary server.

This configuration work should be done at the same time HA is being set up: that is, after the secondary server is installed but before HA registration on the primary server. It must be completed before a failover so that the chance of losing data is eliminated or reduced. Not using a virtual IP address entails no change to the secondary server install procedure. The primary and secondary servers still need to be provisioned with their individual IP addresses, as normal.

This workaround is not available to you if you want to use HA with Operations Center. Enabling virtual IP addressing is a firm requirement in this case (see “Enable HA for Operations Center”).

Related Topics

Using Virtual IP Addressing With HA
Planning HA Deployments
Network Throughput Restrictions on HA, on page 878
Using the Campus Model, on page 880
Using the Remote Model, on page 880
Enabling HA for Operations Center

How to Configure HA Between the Primary and Secondary Servers

To enable HA, you must configure HA on the primary server. The primary server does not need any configuration during the installation to participate in HA configuration. You need to have the following information before configuring the primary server:

- The IP address or host name of the secondary HA server, which you have already installed and configured (installing the secondary server is described in the *Cisco Evolved Programmable Network Manager Installation Guide*).

- The authentication key you set during installation of the secondary server.
- (Optional) One or more email addresses, to which notifications are to be sent.
- The Failover type (see Automatic Versus Manual Failover, on page 881).

If you plan to use virtual IP addressing, see Using Virtual IP Addressing With HA, on page 882).

If you plan to use NIC teaming interface, see NIC Teaming with HA, on page 886 for more information.

The following steps explain how to configure HA on a primary server. Follow the same steps while reconfiguring HA.

Before you begin

If you plan to use multiple virtual IP addresses, ensure that you configure them using CLI before this procedure. See Multiple Virtual IP Addressing with HA, on page 883 for more information.

Note If you plan to use only one virtual IP address, you can configure it from the Cisco EPN Manager UI during HA registration. There is no need to configure it through CLI.

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** and then complete the following fields:

a. **Secondary Server**: Enter the IP address or the host name of the secondary server.

Note It is recommended that you use a DNS server for resolving the host name to IP address. If you're using the "/etc/hosts" file instead of DNS server, enter the secondary IP address instead of host name.

b. **Authentication Key**: Enter the authentication key password you set during the secondary server installation.

c. **Email Address** (Optional): Enter the address (or comma-separated list of addresses), to which notification about HA state changes should be mailed. If you have already configured email notifications using the Mail Server Configuration page, the email addresses you enter here will be appended to the list of addresses already configured for the mail server.

d. **Failover Type**: Select either **Manual** or **Automatic**. We recommend that you select **Manual**.

Step 4 (Ignore this step and go to Step 5 if you have already configured the virtual IP address using CLI) If you are using the virtual IP feature, then select the **Enable Virtual IP** check box and complete the additional fields as follows:

a. **IPV4 Virtual IP**: Enter the virtual IPv4 address that you want both HA servers to use.

b. **IPV6 Virtual IP**: (Optional) Enter the IPv6 address that you want both HA servers to use.

Note Virtual IP addressing does **not** work unless both the servers are on the same subnet.

Step 5 Click **Check Readiness** to ensure if the HA-related environmental parameters are ready for the configuration.

For more details, see Check Readiness for HA Registration/Configuration, on page 888.

Note The readiness check doesn't block the HA configuration. You can configure HA even if some of the tests do not pass.

Step 6 Click **Save** to save your changes. Cisco EPN Manager initiates the HA configuration process. When the configuration is successfully complete, **Configuration Mode** displays the value **HA Enabled**.

Note If FTP or TFTP service is running on the primary server, you must restart the secondary server after the configuration is complete to ensure that failover does not fail.

Key points to note:

- The High availability feature does not manage virtual IP addresses added after HA registration. It is recommended that you do not add virtual IP addresses after HA registration.
- HA registration failure deletes all configured virtual IP addresses. You need to configure them again before HA registration.
- High availability fails if you remove the virtual IP addresses after high availability has been enabled.
- When a fiber is disconnected on a circuit, restore operation is triggered. During restoration if HA switch-over occurs between primary and secondary servers, **Discovery** state of the circuit *might* go to **Partial** on the switched over EPNM server. You can resolve this by manually syncing the devices or scheduling synchronization every night.
- To modify virtual IP addresses you have already configured:
  1. Remove the existing HA configuration.
  2. Configure the virtual IP addresses.
  3. Perform HA registration again.

NIC Teaming with HA

With Cisco EPN Manager, you must designate the NIC teaming interface as the "northbound interface" to be used for HA deployment. NIC teaming designation can be configured from CLI.

NIC teaming interface configuration and the designation as the "northbound interface" must be configured identically on primary and secondary servers as a prerequisite for HA deployment.

Note If the NIC teaming interface is configured with eth0 as a member, then the NIC teaming interface is automatically selected for NBI.

If the NIC teaming interface is configured without eth0 as a member, then the NIC teaming interface will be used only for SBI.

To designate NIC teaming interface as the "northbound interface" from CLI, follow these steps:

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

Step 2 Enter the following command at the prompt:

```
ncs ha northbound interface Team <0-2>
```

Step 3 Specify the NIC teaming interface number that is to be designated as “northbound interface” for HA deployment.

Step 4 Save the configuration:

```
write memory
```

Step 5 (Optional) Verify the configuration by running this command:

```
show running-config
```

Note The above procedure is certified only for NIC teaming interface.

Any other “northbound interface” configuration may work, but is not officially certified.

Configure an SSO Server in an HA Environment

Single Sign-On (SSO) authentication is used to authenticate and manage users in a multi-user, multi-repository environment. SSO is responsible for storing and retrieving the credentials that are used for logging into different systems. You can set up a Cisco EPN Manager as the SSO server for other instances of Cisco EPN Manager.

To configure an SSO server in the high-availability environment, choose one of the procedures listed in the Table 61: SSO Configuration in a HA Deployment. See these topics for more information:

- To configure the SSO server, see Add a RADIUS or TACACS+ Server to Cisco EPN Manager, on page 824.
- To configure the HA servers, see the Cisco Evolved Programmable Network Manager Installation Guide.

Table 61: SSO Configuration in a HA Deployment

SSO Configuration	Setup SSO Server	Sever Failover Scenario	SSO Server Failure Scenario
SSO as a standalone server	1. Configure the standalone SSO server. 2. Configure the primary and secondary HA servers.	When the primary server fails, the secondary server is activated. All machines that are connected to the primary server will be redirected to the secondary server.	When the SSO server fails, SSO functionality is disabled. Cisco EPN Manager will use local authentication.

SSO Configuration	Setup SSO Server	Sever Failover Scenario	SSO Server Failure Scenario
SSO on the secondary Server	1. Configure one server to be the SSO server and the primary server (in other words, the primary server will also be the SSO server). 2. Configure the secondary HA server.	When the primary server fails, the secondary server is activated. All machines that are connected to primary server will not be redirected to the secondary server (because SSO is configured on the primary server).	When the SSO (primary) server fails, the secondary server can be set as the failback option for SSO. This enables all instances to connect to the secondary server. If the secondary server is not set as the SSO server failback option, Cisco EPN Manager will use local authentication.

Check Readiness for HA Registration/Configuration

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

An approximate of 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.

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 are displayed. The screen shows 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 62: Checklist name and description

Checklist Test Name	Test Description
SYSTEM - Check CPU Count	This validates the CPU count in primary and secondary server. The CPU count in primary server can be less than or equal to the secondary server.

DATABASE - LISTENER STATUS	This checks if the database listeners are up and running in both primary and secondary server. If there is a failure, the test restarts and reports the status. This checks if all the wcs instances exist under oracle "listener.ora" file. This is executed in both primary and secondary server.
DATABASE - CHECK MEMORY TARGET	This checks for "/dev/shm" database memory target size for HA setup.
DATABASE - CHECK LISTENER CONFIG CORRUPTION	This checks for all the database instances exist under database listener configuration. This is executed in both primary and secondary server.
SYSTEM - HEALTH MONITOR STATUS	This checks whether the health monitor process is running in both primary and secondary server.
SYSTEM - CHECK DISK IOPS	This validates the disk IOPS in both primary and secondary server. The minimum expected disk IOPS is 200 MBps.
NETWORK - CHECK FIREWALL FOR DATABASE PORT ACCESSIBILITY	This checks if the database port 1522 is open in the system firewall. If the port is disabled, the test grants permission for 1522 in the ip tables list.
NETWORK - CHECK NETWORK INTERFACE BANDWIDTH	This checks if the eth0 interface speed matches the recommended speed of 100 Mbps in both primary and secondary server. This test will not measure network bandwidth by transmitting data between primary and secondary server.
NETWORK - CHECK NETWORK BANDWIDTH SPEED	This checks if the network bandwidth speed matches the recommended speed of 100 Mbps in both primary and secondary server. This test measures the network bandwidth by transmitting data between primary and secondary server.
DATABASE - CHECK ONLINE STATUS	This checks if the database files status is online and accessible in both primary and secondary server.
DATABASE - CHECK TNS CONFIG CORRUPTION	This validates if the tnsping is successful in both primary and secondary server.
DATABASE - TNS REACHABILITY STATUS	This checks if all the wcs instances exist under oracle "listener.ora" file. This is executable in both primary and secondary server.

DATABASE - VALIDATE STANDBY DATABASE INSTANCE	This validates if the standby database instance (stbywcs) is available in both primary and secondary server.
SYSTEM - CHECK RAM SIZE	This checks if the disk size of primary server less than or equal to secondary server.
SYSTEM - CHECK SERVER PING REACHABILITY	This ensures that the primary server can run ping check with the remote (secondary) server.

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

Note The validation failback and failover events during Check Readiness will be sent to the Alarms and Events page; whereas, the registration failure event will not be present in the Alarms and Evens page.

How to Patch HA Servers

You can download and install UBF patches for your HA servers in one of the following ways, depending on your circumstances:

- Install the patch on HA servers that are not currently paired. Cisco recommends this method if you have not already set up HA for Cisco EPN Manager.
- Install the patch on existing paired HA servers using manual failover. This is the method Cisco recommends if you already have HA set up.
- Install the patch on existing paired HA servers using automatic failover.

For details on each method, see the Related Topics.

Related Topics

How to Patch New HA Servers, on page 890
How to Patch Paired HA Servers, on page 892

How to Patch New HA Servers

If you are setting up a new Cisco EPN Manager High Availability (HA) implementation and your new servers are not at the same patch level, follow the steps below to install patches on both servers and bring them to the same patch level.

Step 1 Download the patch and install it on the primary server:

a) Point your browser to the software patches listing for Cisco EPN Manager (see Software Download).
b) Click the **Download** button for the patch file you need to install (the file name ends with a UBF file extension), and save the file locally.
c) Log in to the primary server using an ID with administrator privileges and choose **Administration > Licenses and Software Updates > Software Update**.
d) Click the **Upload** link at the top of the page and browse to the location where you saved the patch file.
e) Select the UBF file and click **OK** to upload the file.

f) Use one of the following options to upload the UBF file.

1. Upload from local computer
   - Click the **Upload from local computer** radio button in the **Upload Update** window.
   - Click **Browse**, navigate to the file, and click **OK**. After the successful upload, the software will appear under the **Files** tab.
2. Copy from server's local disk
   - Click the **Copy from server's local disk** radio button in the **Upload Update** window.
   - Click **Select** , select the UBF file form the **Select file from local disk** pop-up and click **Select**. After the successful upload, the software will appear under the **Files** tab.

g) When the upload is complete: On the Software Upload page, verify that the Name, Published Date and Description of the patch file are correct.
h) Select the patch file and click **Install**.
i) Click **Yes** in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.
j) After the installation is complete on the primary server, verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

Step 2 Install the same patch on the secondary server:

a) Access the secondary server’s Health Monitor (HM) web page by pointing your browser to the following URL:

https://*ServerIP***:8082**

where *ServerIP* is the IP address or host name of the secondary server.

b) You will be prompted for the secondary server authentication key. Enter it and click **Login**.
c) Click the HM web page’s **Software Update** link. You will be prompted for the authentication key a second time. Enter it and click **Login** again.
d) Click **Upload Update File** and browse to the location where you saved the patch file.
e) Select the UBF file and click **OK** to upload the file.
f) Click the **Upload** link at the top of the page.
g) Use one of the following options to upload the UBF file.

1. Upload from local computer
   - Click the **Upload from local computer** radio button in the **Upload Update** window.
   - Click **Browse**, navigate to the file, and click **OK**. After the successful upload, the software will appear under the **Files** tab.
2. Copy from server's local disk
   - Click the **Copy from server's local disk** radio button in the **Upload Update** window.
   - Click **Select** , select the UBF file form the **Select file from local disk** pop-up and click **Select**. After the successful upload, the software will appear under the **Files** tab.

h) When the upload is complete: On the Software Upload page, confirm that the Name, Published Date and Description of the patch file are correct.

i) Select the patch file and click **Install**.
j) Click **Yes** in the warning pop-up. When the installation is complete, the server will restart automatically. The restart typically takes 15 to 20 minutes.
k) After the installation is complete on the secondary server, verify that the Status of Updates table on the Software Update page shows “Installed” for the patch.

Step 3 Verify that the patch status is the same on both servers, as follows:

a) Log in to the primary server and access its Software Update page as you did in step 1, above. The **Status** column should show **Installed** for the installed patch.
b) Access the secondary server’s Health Monitor page as you did in step 2, above. The **Status** column should show **Installed** for the installed patch

Step 4 Register the servers.

For more information, see Software Download and Stop and Restart Cisco EPN Manager, on page 769.

How to Patch Paired HA Servers

If your current Cisco EPN Manager implementation has High Availability servers that are not at the same patch level, or you have a new patch you must install on both your HA servers, follow the steps below.

Patching paired HA servers is not supported. You will receive a popup error message indicating that you cannot perform an update on Cisco EPN Manager servers while HA is configured. So, you must first disconnect the primary and secondary servers before attempting to apply the patch.

1. Follow the steps in “Remove HA Via the GUI” (see Related Topics) to disconnect the primary and secondary servers.
2. Follow the steps in “How to Patch New HA Servers” to apply the patch.
3. Follow the steps in “Set Up High Availability” to restore your HA configuration.

Related Topics

Set Up High Availability
Checking High Availability Status
Remove HA Via the GUI, on page 912
How to Patch New HA Servers, on page 890

Monitor HA Status and Events

These topics describe how to monitor the overall health of the HA environment:

- Use the Health Monitor Web Page, on page 893
- HA Configuration Modes, on page 908
- HA States and Transitions, on page 908
- Check HA Status and Overall Health, on page 894
- View and Customize HA Events, on page 895

• Use HA Error Logging, on page 895

Use the Health Monitor Web Page

The Health Monitor is one of the main components that manage the HA operations. Health Monitor instances run on both servers as an application process, with its own web page on each server. It performs the following functions:

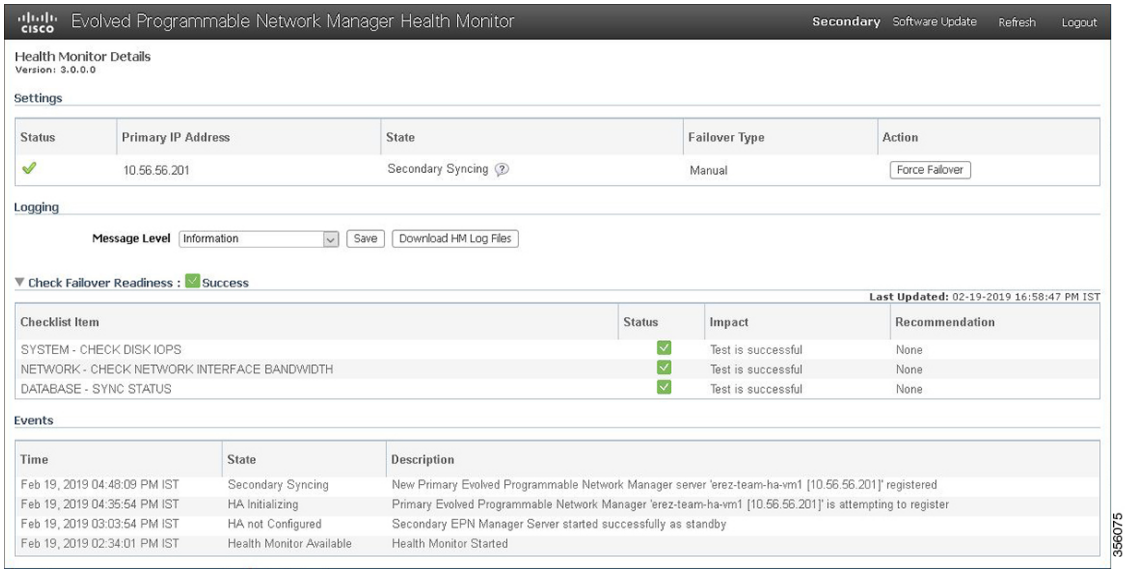
- Synchronizes database and configuration data related to HA (this excludes databases that synchronize separately using Oracle Data Guard).
- Exchanges heartbeat messages between the primary and secondary servers every 5 seconds, to ensure communications are maintained between the servers. If the healthy server does not receive 3 consecutive heartbeats from the other redundant server, it waits for 10 seconds. The healthy server then attempts to open a web URL in the redundant server. If this attempt fails, the healthy server becomes the active server.
- Checks the available disk space on both servers at regular intervals and generates events when storage space runs low.
- Manages, controls, and monitors the overall health of the linked HA servers. If there is a failure on the primary server, the Health Monitor activates the secondary server.

After you have completed HA configuration successfully, you can access the Health Monitor web page from the primary or secondary server by entering the following URL on your browser:

`https://`*`ServerIP`***`:8082`**

where *ServerIP* is the primary or secondary server's IP address or host name.

The following example shows a Health Monitor web page for a secondary server in the **Secondary Syncing** state.



1	Settings—Displays the Health Monitor state and configuration detail in five separate sections.	2	Status—Indicates the current functional status of the HA setup (a green check mark indicates HA is enabled and working).
3	Events—Displays the current HA-related events in chronological order, with the most recent events at the top.	4	Primary/Secondary IP address—Displays the IP address of the paired servers. Because this Health Monitor instance is running on the secondary server, it shows the IP address of the primary server.
5	Download—Lets you download the Health Monitor log files.	6	State—Shows the current state of the server on which this Health Monitor instance is running (in this case, the secondary server).
7	Message Level—Indicates the current logging level, which you can change (Error, Informational, or Trace). You must click **Save** to change the logging level.	8	Title bar—Identifies the HA server whose Health Monitor web page you are viewing, along with the Refresh and Logout buttons. Note that the Software Update is only displayed for secondary servers.
9	Failover Type—Shows whether you have Manual or Automatic failover configured.	10	Action—Shows the actions you can perform, such as failover or failback. Only the available actions are displayed here.
11	Check Failover Readiness—Shows the outcome of the disk speed, network interface bandwidth and DB sync status checks after the HA configuration is enabled.		

Note The **Check Readiness** does not block failover to the secondary(either automatic or manual).

Check HA Status and Overall Health

You can use the Cisco EPN Manager web GUI or CLI to check HA status. Either of these approaches will list the state of the server. States are described in HA States and Transitions, on page 908.

To check the HA status from the web GUI, do one of the following:

- From the Cisco EPN Manager web GUI—Choose **Administration** > **Settings** > **High Availability**, then choose **HA Status**. The current HA status and the event states are displayed.
- From the Health Monitor. See Use the Health Monitor Web Page, on page 893.

To check HA status from the CLI, log into either server as a CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765). The **ncs ha status** command provides a HA-specific output similar to the below example:

```
ncs ha status
[Role] Secondary [Primary Server] cisco-ha1(192.0.2.133) [State] Secondary Active [Failover
 Type] Manual
```

Use the **ncs status** command to check the Health Monitor and other server processes. You will see an output similar to the following example:

```
ncs status
Health Monitor Server is running. ( [Role] Primary [State] Primary Active )
Database server is running
FTP Service is disabled
TFTP Service is disabled
NMS Server is running.
SAM Daemon is running ...
DA Daemon is running ...
```

View and Customize HA Events

HA-related alarms are listed in the Alarms and Events table. A list of these alarms is provided in Cisco Evolved Programmable Network Manager Supported Alarms. The following procedure explains how to view these alarms in the web GUI.

If desired, you can also:

- Adjust the severity for these alarms
- Configure notifications for these alarms

For more information, see Work With Server Internal SNMP Traps That Indicate System Problems, on page 776.

To view HA-related alarms:

Step 1 Choose **Monitor** > **Monitoring Tools** > **Alarms and Events**, then click the **Alarms** tab.

Step 2 Choose **Quick Filter** from the **Show** drop-down list at the top right of the table.

Step 3 In the **Message** field, enter **High Availability**.

Use HA Error Logging

To save disk space and maximize performance, HA error logging is disabled by default. If you are having trouble with HA, complete the following procedure to enable error logging and examine the log files.

Step 1 Launch the Health Monitor on the server that is having trouble (see Use the Health Monitor Web Page, on page 893).

Step 2 In the **Logging** area, select the error-logging level from the **Message Level** drop-down list and then click **Save**.

Step 3 Download the log files you want to examine:

a. Click **Download**.

A .zip file is copied to your default download location.

b. Extract the log files and use any ASCII text editor to view them.

Trigger Failover

Failover activates the secondary server in response to a failure detected on the primary server.

The Health Monitor detects failure conditions using the heartbeat messages exchanged between the two HA servers. The heartbeat messages are sent every 5 seconds, and if the primary server is not responsive to three consecutive heartbeat messages from the secondary server, the Health Monitor deems the primary server to have failed. During the health check, the Health Monitor also checks the application process status and database health. If there is no proper response to these checks, these are also treated as having failed.

The HA system in the secondary server takes about 15 seconds to detect a process failure on the primary server. If the secondary server is unable to reach the primary server due to a network issue, it might take more time to discover the failure and initiate a failover. In addition, it may take additional time for the application processes on the secondary server to be fully operational.

As soon as the Health Monitor detects a failure, it sends an e-mail notification. The e-mail includes the failure status along with a link to the secondary server's Health Monitor web page. If HA is configured for automatic failover, the secondary server will activate automatically.

To perform a manual failover:

Before you begin

- Check the state of the primary and secondary servers.
- Validate the connectivity between the two servers.
- If you are not using virtual IP addresses, make sure all devices are configured to forward traps and syslogs to both servers.

Step 1 Access the secondary server's Health Monitor web page using the web link given in the email notification, or by entering the following URL on your browser:

`https://ServerIP:8082`

Step 2 Click **Failover**.

Trigger Failback

Failback is the process of re-activating the primary server once it is back online. It also transfers Active status from the secondary server to the primary server, and stops active network monitoring processes on the secondary server.

When a failback is triggered, the secondary server replicates its current database information and updated files to the primary server. The time it takes to complete the failback from the secondary server to the primary server will depend on the amount of data that needs to be replicated and the available network bandwidth.

After the data is replicated successfully, HA changes the state of the primary server to **Primary Active** and the state of the secondary server to **Secondary Syncing**.

During failback, the availability of the secondary server depends on whether the Cisco EPN Manager was re-installed on the primary server after the failover, as follows:

- If Cisco EPN Manager was re-installed on the primary server after the failover, a full database copy will be required and the secondary server will not be available during the failback process.
- If Cisco EPN Manager was not re-installed with primary server, the secondary server is available, except during the period when processes are started on the primary server and stopped on the secondary server. Both servers' Health Monitor web pages are accessible for monitoring the progress of the failback. Additionally, users can also connect to the secondary server to access all normal functionalities.

You must always trigger failback manually, as described in the procedure below. Note:

- Do not initiate configuration or provisioning activity while the failback is in progress.
- After a successful failback, the secondary server will go down and control will switch over to the primary server. During this process, Cisco EPN Manager will be inaccessible to the users for a few moments.

Before you begin

- Check the state of the primary and secondary servers.
- Validate the connectivity between the two servers.
- If you are not using virtual IP addresses, make sure all devices are configured to forward traps and syslogs to both servers.
- If you have re-installed Cisco EPN Manager on the primary server and you are using offline geo maps, you must re-install the geo maps resources on the primary server before triggering failback. See the Cisco Evolved Programmable Network Manager Installation Guide.

Step 1 Access the secondary server's Health Monitor web page using the link given in the e-mail notification, or by entering the following URL on your browser:

`https://ServerIP:8082`

Step 2 Click **Failback**.

Force Failover

A forced failover is the process of making the secondary server active while the primary server is still up. You will want to use this option when, for example, you want to test that your HA setup is fully functional.

Forced failover is available to you only when the primary is active, the secondary is in the "Secondary syncing" state, and all processes are running on both servers. Forced failover is disabled when the primary server is down. In this case, only the normal Failover is enabled.

Once the forced failover completes, the secondary server will be active and the primary will restart in standby automatically. You can return to an active primary server and standby secondary server by triggering a normal failback.

Step 1 Access the secondary server's Health Monitor web page using the steps in Use the Health Monitor Web Page.

Step 2 Trigger the forced failover by clicking the **Force Failover** button. The forced failover will complete in 2 to 3 minutes.

Respond to Other HA Events

All the HA related events are displayed on the HA Status page, the Health Monitor web pages, and under the Cisco EPN Manager Alarms and Events page. Most events require no response from you other than triggering failover and failback. A few events are more complex, as explained in the following topics:

HA Registration Fails

If HA registration fails, you will see the following HA state-change transitions for each server:

Primary HA State Transitions...	Secondary HA State Transitions...
From: HA Initializing	From: HA Initializing
To: HA Not Configured	To: HA Not Configured

To recover from failed HA registration, follow the steps below.

Step 1 Use ping and other tools to check the network connection between the two Cisco EPN Manager servers. Confirm that the secondary server is reachable from the primary, and vice versa.

Step 2 Check that the gateway, subnet mask, virtual IP address (if configured), server hostname, DNS, NTP settings are all correct.

Step 3 Check that the configured DNS and NTP servers are reachable from the primary and secondary servers, and that both are responding without latency or other network-specific issues.

Step 4 Check that all Cisco EPN Manager licenses are correctly configured.

Step 5 Once you have remedied any connectivity or setting issues, retry the steps in How to Configure HA Between the Primary and Secondary Servers, on page 884.

Network is Down (Automatic Failover)

If there is a loss of network connectivity between the two Cisco EPN Manager servers, you will see the following HA state-change transitions for each server, assuming that the Failover Type is set to “Automatic”:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Lost Secondary	To: Secondary Lost Primary
To: Primary Lost Secondary	To: Secondary Failover
To: Primary Lost Secondary	To: Secondary Active

You get an email notification that the secondary is active.

Step 1 Check on and restore network connectivity between the two servers. Once network connectivity is restored and the primary server can detect that the secondary is active, all services on the primary will be restarted and made passive automatically. You will see the following state changes:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Lost Secondary	From: Secondary Active
To: Primary Failover	To: Secondary Active
To: Primary Syncing	To: Secondary Active

Step 2 Trigger a failback from the secondary to the primary. You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Syncing	From: Secondary Active
To: Primary Failback	To: Secondary Failback
To: Primary Failback	To: Secondary Post Failback

Primary HA State Transitions...	Secondary HA State Transitions...
To: Primary Active	To: Secondary Syncing

Network is Down (Manual Failover)

If there is a loss of network connectivity between the two Cisco EPN Manager servers, you will see the following HA state-change transitions for each server, assuming that the Failover Type is set to “Manual”:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Lost Secondary	To: Secondary Lost Primary

You will get email notifications that each server has lost the other.

Step 1 Check on and, if needed, restore the network connectivity between the two servers.

You will see the following state changes once network connectivity is restored.:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Lost Secondary	From: Secondary Lost Primary
To: Primary Active	To: Secondary Syncing

No administrator response is required.

Step 2 If network connection cannot be restored for any reason, use the HM web page for the secondary server to trigger a failover from the primary to the secondary server. You will see the following state changes:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Lost Secondary	From: Secondary Lost Primary
To: Primary Lost Secondary	To: Secondary Failover
To: Primary Failover	To: Secondary Active

You will get an email notification that the secondary server is now active.

Step 3 Check and restore network connectivity between the two servers. Once network connectivity is restored and the primary server detects that the secondary server is active, all services on the primary server will be restarted and made passive. You will see the following state changes:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Lost Secondary	From: Secondary Active
To: Primary Failover	To: Secondary Active

Primary HA State Transitions...	Secondary HA State Transitions...
To: Primary Syncing	To: Secondary Active

Step 4 Trigger a failback from the secondary to the primary.

You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Syncing	From: Secondary Active
To: Primary Failback	To: Secondary Failback
To: Primary Failback	To: Secondary Post Failback
To: Primary Active	To: Secondary Syncing

Process Restart Fails (Automatic Failover)

The Cisco EPN Manager Health Monitor process is responsible for attempting to restart any Cisco EPN Manager server processes that have failed. Generally speaking, the current state of the primary and secondary servers should be “Primary Active” and “Secondary Syncing” at the time any such failures occur.

If HM cannot restart a critical process on the primary server, then the primary server is considered to have failed. If your currently configured Failover Type is “automatic”, you will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Uncertain	To: Secondary Lost Primary
To: Primary Failover	To: Secondary Failover
To: Primary Failover	To: Secondary Active

When this process is complete, you will get an email notification that the secondary server is now active.

Step 1 Restart the primary server and ensure that it is running. Once the primary is restarted, it will be in the state “Primary Syncing”. You will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Failover	From: Secondary Active
To: Primary Preparing for Failback	To: Secondary Active
To: Primary Syncing	To: Secondary Active

Step 2 Trigger a failback from the secondary to the primary. You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Syncing	From: Secondary Active
To: Primary Failback	To: Secondary Failback
To: Primary Failback	To: Secondary Post Failback
To: Primary Active	To: Secondary Syncing

Process Restart Fails (Manual Failover)

The Cisco EPN Manager Health Monitor process is responsible for attempting to restart any Cisco EPN Manager server processes that have failed. Generally speaking, the current state of the primary and secondary servers should be “Primary Active” and “Secondary Syncing” at the time any such failures occur. If HM cannot restart a critical process on the primary server, then the primary server is considered to have failed. You will receive an email notification of this failure. If your currently configured Failover Type is “Manual”, you will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Uncertain	To: Secondary Lost Primary

Step 1 Trigger on the secondary server a failover from the primary to the secondary. You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Uncertain	From: Secondary Syncing
To: Primary Failover	To: Secondary Failover
To: Primary Failover	To: Secondary Active

Step 2 Restart the primary server and ensure that it is running. Once the primary server is restarted, the primary’s HA state will be “Primary Syncing”. You will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Failover	From: Secondary Active
To: Primary Preparing for Failback	To: Secondary Active
To: Primary Syncing	To: Secondary Active

Step 3 Trigger a failback from the secondary to the primary. You will then see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Syncing	From: Secondary Active
To: Primary Failback	To: Secondary Failback
To: Primary Failback	To: Secondary Post Failback
To: Primary Active	To: Secondary Syncing

Primary Server Restarts During Synchronization (Manual Failover)

If the primary Cisco EPN Manager server is restarted while the secondary server is syncing, you will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Alone	To: Secondary Lost Primary
To: Primary Active	To: Secondary Syncing

The “Primary Alone” and “Primary Active” states occur immediately after the primary comes back online. No administrator response should be required.

Secondary Server Restarts During Synchronization

If the secondary Cisco EPN Manager server is restarted while syncing with the primary server, you will see the following state transitions:

Primary HA State Transitions...	Secondary HA State Transitions...
From: Primary Active	From: Secondary Syncing
To: Primary Lost Secondary	From: Secondary Lost Primary
To: Primary Active	To: Secondary Syncing

No administrator response should be required.

Both HA Servers Are Down

If both the primary and secondary servers are down at the same time, you can recover by bringing them back up in the correct order, as explained in the steps below.

Step 1 Restart the secondary server and the instance of Cisco EPN Manager running on it. If for some reason you cannot restart the secondary server, see “Both HA Servers Are Down and Secondary Will Not Restart” in Related Topics.

Step 2 When the Cisco EPN Manager is running on the secondary, access the secondary server’s Health Monitor web page. You will see the secondary server transition to the state “Secondary Lost Primary”.

Step 3 Restart the primary server and the instance of Cisco EPN Manager running on it. When the Cisco EPN Manager is running on the primary, the primary will automatically sync with the secondary. To verify this, access the primary server’s Health Monitor web page. You will see the two servers transition through the following series of HA states:

Primary HA State Transitions...	Secondary HA State Transitions...
To: Primary Lost Secondary	To: Secondary Lost Primary
To: Primary Active	To: Secondary Syncing

Related Topics

Accessing the Health Monitor Web Page
Responding to Other HA Events

Both HA Servers Are Powered Down

If both the primary and secondary servers are powered down at the same time, you can recover by bringing them back up in the correct order, as explained in the steps below.

Step 1 Power on the secondary server and the Cisco EPN Manager instance running on it. The secondary HA restart will fail at this state because the primary server is not reachable. However, the secondary server's HM process will be running (with an error).

Step 2 When Cisco EPN Manager is running on the secondary server, access the secondary server's HM web page (see Use the Health Monitor Web Page, on page 893). You will see the secondary server transition to the **Secondary Lost Primary** state.

Step 3 Power on the primary server and the Cisco EPN Manager instance running on it.

Step 4 When Cisco EPN Manager is running on the primary server, the primary server will automatically begin syncing with the secondary server. To verify this, access the primary server's HM web page. You will see the two servers transition through the following series of HA states:

Primary HA State Transitions...	Secondary HA State Transitions...
To: Primary Lost Secondary	To: Secondary Lost Primary
To: Primary Active	To: Secondary Syncing

Step 5 Restart the secondary server and the Cisco EPN Manager instance running on it. This is required because not all processes will be running on the secondary server at this point.

If for some reason you cannot restart the secondary server, see Both HA Servers Are Down and Secondary Server Will Not Restart, on page 905.

Step 6 When Cisco EPN Manager finishes restarting on the secondary server, all processes should be running. Verify this by running the **ncs ha status** command.

Both HA Servers Are Down and Secondary Server Will Not Restart

If both HA servers are down at the same time and the secondary server will not restart, you will need to remove the HA configuration from the primary server in order to use it as a standalone server until you can replace the secondary server.

The following steps assume that you have already tried and failed to restart the secondary server.

Step 1 Attempt to restart the primary instance of Cisco EPN Manager. If the primary server is able to restart at all, the restart will abort with an error message indicating that you must remove the HA configuration.

Step 2 Open a CLI session with the primary server (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Step 3 Enter the following command to remove the HA configuration on the primary server:

```
ncs ha remove
```

Note Once you remove the HA configuration, you need to reinstall the secondary server since the primary will no longer be able to register with the former secondary.

Step 4 Confirm that you want to remove the HA configuration.

You should now be able to restart the primary instance of Cisco EPN Manager without receiving an error message, and use it as a standalone server. When you are able to replace the secondary server, proceed as explained in How to Configure HA Between the Primary and Secondary Servers, on page 884.

How to Replace the Primary Server

Under normal circumstances, the state of your primary server will be **Primary Active** and your secondary server will be **Secondary Syncing**. If the primary server fails for any reason, a failover to the secondary will take place (automatically or manually).

You may find that restoring full HA access requires you to re-install the primary server using new hardware. If this happens, you can follow the steps below to bring up the new primary server without losing any data.

Before you begin

Make sure you have the password (authentication key) that was set when HA was configured on the secondary server. You will need it for this procedure.

Step 1 Ensure that the secondary server is in the **Secondary Active** state. If the primary server is configured for manual failover, you will need to trigger failover to the secondary server (see Trigger Failover, on page 896).

Step 2 Ensure that the old primary server you are replacing has been disconnected from the network.

Step 3 Ensure that the new primary server is ready for use. This will include connecting it to the network and configuring it similar to the old primary server (IP address, subnet mask, and so forth). You will need to enter the same authentication key that you entered when installing HA on the secondary server.

Step 4 Ensure that both the primary and secondary servers are at the same patch level and if you want to replace the primary server, then you must:

a) Ensure the primary and secondary server are in TOFU Mode by executing the following command in the secondary server CLI:

admin# ncs certvalidation certificate-check trust-on-first-use trustzone system

b) Login to Secondary server admin CLI.

c) Execute the following command in the secondary server CLI:

admin# ncs certvalidation tofu-certs deletecert host <primaryserver's-IP-address appended with "_8082">

For example: **ncs certvalidation tofu-certs deletecert host 10.56.58.91_8082**

This is required to re-establish the communication between the Primary and Secondary servers.

Step 5 Update the IP table entries as listed below:

- On Primary - Add Secondary IP address and Virtual IP address (if configured) in iptables for 1522 port.
- On Secondary - Add Primary IP address and Virtual IP address (if configured) in iptables for 1522 port.

Example:

```
iptables -A INPUT -s IP address -p tcp --dport 1522 -j ACCEPT
iptables -A INPUT -s IP address -j ACCEPT
```

Step 6 Trigger a failback from the secondary server to the newly-installed primary server. During failback to the new primary HA server, a full database copy will be performed, so this operation will take time to complete depending on the available bandwidth and network latency. You will see the two servers transition through the following series of HA states:

Primary HA State Transitions...	Secondary HA State Transitions...
From: HA not configured	From: Secondary Active
To: Primary Failback	To: Secondary Failback
To: Primary Failback	To: Secondary Post Failback
To: Primary Active	To: Secondary Syncing

How to Recover From Split-Brain Scenario

In a split-brain scenario, both the primary and secondary servers become active at the same time, perhaps due to a network outage or a link that temporarily goes down. However, because the primary server constantly checks the secondary server, when the connection is reestablished, the primary server will go down due to the secondary server being active.

The possibility of data loss always exists on the rare occasions when a “split-brain scenario” occurs. In this case, you can choose to save the newly added data on the secondary and forget the data that was added on the primary, as explained in the following steps.

Step 1 Once the network is up, and the secondary server is up, the primary will restart itself automatically, using its standby database. The HA status of the primary server will be, first, “Primary Failover” transitioning to “Primary Syncing”. You can verify this by logging on to the primary server’s Health Monitor web page.

Step 2 Once the primary server’s status is “Primary Syncing, confirm that a user can log into the secondary server’s Cisco EPN Manager page using the web browser (for example, https://server-ip-address:443). Do not proceed until you have verified this.

Step 3 Once access to the secondary is verified, initiate a failback from the secondary server's Health Monitor web page (see Trigger Failback, on page 896). You can continue to perform monitoring activities on the secondary server until the switchover to the primary is completed.

Secondary Server Goes Down

In this scenario, the secondary server is acting as a standby server and it goes down.

To get the secondary server up and running again:

Step 1 Power on the secondary server.

Step 2 Start Cisco EPN Manager on the secondary server.

Step 3 On the primary server, verify that the primary server's HA status changes from "Primary Lost Secondary" to "Primary Active." Go to **Administration > Settings > High Availability > HA Configuration**.

Step 4 Log into the secondary server's Health Monitor page by entering the following URL in your browser: **https://*serverIP*:8082**.

Step 5 Verify that the secondary server's HA status changes from "Secondary Lost Primary" to "Secondary Syncing."
No further action is required once the above statuses are displayed. However, if the HA status does not change, the secondary server cannot be recovered automatically. In this case, continue with the following steps.

Step 6 Remove the HA configuration on the primary server. Go to **Administration > Settings > High Availability > HA Configuration** and click **Remove**.

Step 7 Register the secondary server with the primary server. See How to Configure HA Between the Primary and Secondary Servers, on page 884.
If HA registration is successful, no further action is required. However, if HA registration is unsuccessful, it indicates that the secondary server might have suffered hardware/software loss. In this case, continue with the following steps.

Step 8 Remove the HA configuration on the primary server.

Step 9 Reinstall the secondary server with the same release and patches (if any) as the primary server.

Step 10 Register the secondary server with the primary server. See How to Configure HA Between the Primary and Secondary Servers, on page 884.

How to Resolve Database Synchronization Issues

To resolve the database synchronization issue, when the primary server is in "Primary Active" state and the secondary server is in "Secondary Syncing" state, do the following:

Step 1 Remove HA, see Remove HA Via the CLI, on page 912 and Remove HA Via the GUI, on page 912.

Step 2 After both the primary and secondary servers reaches "HA not configured" state, perform the HA registration. See Set Up High Availability, on page 882

High Availability Reference Information

The following sections supply reference information on HA.

Related Topics

HA Configuration Modes, on page 908
HA States and Transitions, on page 908
High Availability CLI Command Reference, on page 911
Reset the HA Authentication Key, on page 911
Remove HA Via the GUI, on page 912
Remove HA Via the CLI, on page 912
Remove HA During Upgrade, on page 912
Remove HA During Restore, on page 913
Use HA Error Logging, on page 895
Reset the Server IP Address or Host Name, on page 913

HA Configuration Modes

HA configuration modes represent the overall status of the complete HA configuration (as opposed to HA states, which are specific to a server).

Mode	Description
HA Not Configured	HA is not configured on this server.
HA Initializing	HA configuration process between the primary and secondary servers has started.
HA Enabled	HA is enabled between the primary and secondary servers.
HA Alone	Server is running alone because one of the servers is down, out of sync, or unreachable.

HA States and Transitions

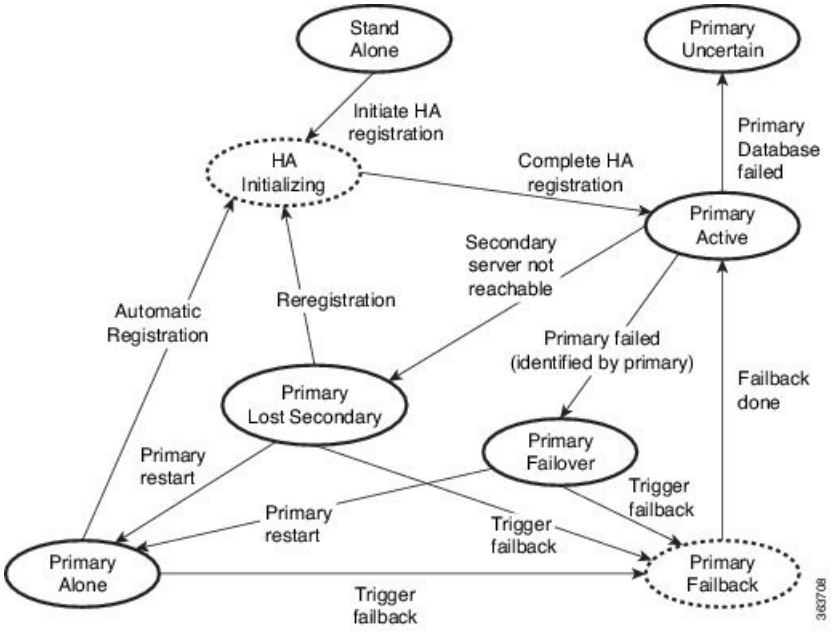
The following table lists the HA states, including those that require no response from you. You can view these states from the HA Status page (**Administration** > **Settings** > **High Availability** > **HA Status**) or from the

Health Monitor. For a list of HA events and instructions for enabling, disabling, and adjusting them, see Customize Server Internal SNMP Traps and Forward the Traps, on page 777.

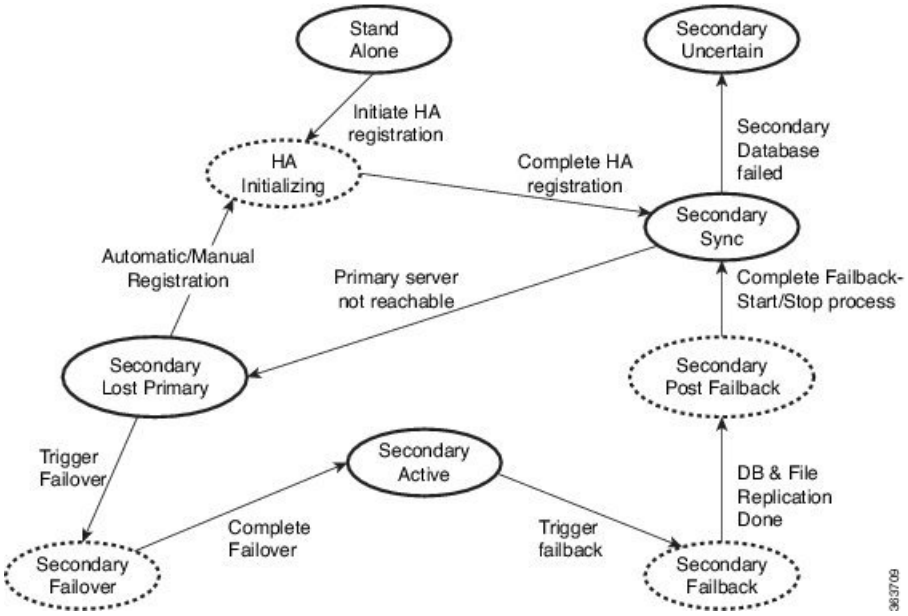
State	Server	Description
Stand Alone	Both	HA is not configured on this server.
Primary Alone	Primary	Primary server has restarted after it lost the secondary server (only Health Monitor is running in this state).
HA Initializing	Both	HA configuration process between the primary and secondary server has started.
Primary Active	Primary	Primary server is now active and is synchronizing with the secondary server.
Primary Database Copy Failed	Primary	Restarted primary server detected a data gap, triggered a data copy from the active secondary server, and the database copy failed. When a primary server is restarted, it always checks to see if a data gap has occurred due to the primary server being down for 24 hours or more. This copy rarely fails but if it occurs, all attempts to failback to the primary are blocked until the database copy completes successfully. As soon as it does, the primary state is set to **Primary Syncing**.
Primary Failover	Primary	Primary server detected a failure.
Primary Failback	Primary	User-triggered failback is currently in progress.
Primary Lost Secondary	Primary	Primary server is unable to communicate with the secondary server.
Primary Preparing for Failback	Primary	Primary server has started up in standby mode after a failover (because the secondary server is still active). When the primary server is ready for failback, its state will be set to **Primary Syncing**.
Primary Syncing	Primary	Primary server is synchronizing the database and configuration files from the active secondary server. This occurs after a failover, when primary processes are brought up (and the secondary server is playing the active role).
Primary Uncertain	Primary	Primary server's application processes are not able to connect to its database.
Secondary Alone	Secondary	Primary server is not reachable from secondary server after a primary server restart.
Secondary Syncing	Secondary	Secondary server is synchronizing the database and configuration files from the primary server.
Secondary Active	Secondary	Failover from the primary server to the secondary server has completed successfully.

Secondary Lost Primary	Secondary	Secondary server is not able to connect to the primary server (occurs when the primary fails or network connectivity is lost). For automatic failover, the secondary server will automatically move to the **Secondary Active** state. For Manual failover, you must trigger the failover to make the secondary server active (see Trigger Failover, on page 896).
Secondary Failover	Secondary	Failover triggered and is in progress.
Secondary Failback	Secondary	Failback triggered and database and file replication is in progress.
Secondary Post Failback	Secondary	Failback triggered; associated process stops and restarts are in progress. Database and configuration files have been replicated from the secondary server to the primary server. The primary server status will change to **Primary Active**, and the secondary server HA status will change to **Secondary Syncing**.
Secondary Uncertain	Secondary	Secondary server's application processes cannot connect to the server's database.

The following figure illustrates the primary server HA state changes.



This figure illustrates the secondary server HA state changes.



High Availability CLI Command Reference

The following table lists the CLI commands available for HA management. Log in as admin to run these commands on the primary server (see Connect via CLI, on page 752):

Table 63: High Availability Commands

Command	Description
ncs ha ?	Get help with high availability CLI commands
ncs ha authkey authkey	Update the authentication key for high availability
ncs ha remove	Remove the High Availability configuration
ncs ha status	Get the current status for High Availability

Related Topics

High Availability Reference Information, on page 908

Reset the HA Authentication Key

Users with administrator privileges can change the HA authentication key using the **ha authkey** command. You will need to ensure that the new authorization key meets the password standards.

Step 1 Log in to the primary server as a Cisco EPN Manager CLI admin user (see Establish an SSH Session With the Cisco EPN Manager Server, on page 765).

Step 2 Enter the following at the command line:

ha authkey *newAuthKey*

Where *newAuthKey* is the new authorization key.

Remove HA Via the GUI

The simplest method for removing an existing HA implementation is via the GUI, as shown in the following steps. You can also remove the HA setup via the command line.

Note that, to use this method, you must ensure that the primary Cisco EPN Manager server is currently in the "Primary Active" state. If for any reason the secondary server is currently active, perform a failback and then try to remove the HA configuration after the failback is complete and the secondary's automatic restart has finished.

Step 1 Log in to the primary Cisco EPN Manager server with a user ID that has administrator privileges.

Step 2 Select **Administration > Settings > High Availability > HA Configuration**.

Step 3 Select **Remove**. Removing the HA configuration takes from 3 to 4 minutes.

Once the removal is complete, ensure that the HA configuration mode displayed on the page now reads "HA Not Configured".

Remove HA Via the CLI

If for any reason you cannot access the Cisco EPN Manager GUI on the primary server, administrators can remove the HA setup via the command line, using the steps below.

To use this method, you must ensure that the primary Cisco EPN Manager server is currently in the "Primary Active" state. If for any reason the secondary server is currently active, perform a failback, and then try to remove the HA configuration after the failback is complete and the secondary's automatic restart has finished.

Step 1 Connect to the primary server via CLI. Do not enter "configure terminal" mode.

Step 2 Enter the following at the command line:

admin# **ncs ha remove**. For more information, see Connect via CLI, on page 752.

Related Topics

Remove HA Via the GUI, on page 912
Trigger Failback, on page 896
High Availability Reference Information, on page 908

Remove HA During Upgrade

To upgrade a Cisco EPN Manager implementation that uses HA, follow the steps below.

Step 1 Use the GUI to remove the HA settings from the primary server (see Remove HA Via the GUI, on page 912).

Step 2 Upgrade the primary server as needed.

Step 3 Reinstall the secondary server using the current image.

Note Upgrading the secondary server from the previous version or a beta version is not supported. The secondary server must always be a fresh installation.

Step 4 Once the upgrade is complete, perform the HA registration process again.

Note After upgrade, health monitor page displays the below health monitor event message:

Primary Authentication Key was changed by Admin

For more information, see Connect via CLI, on page 752.

Related Topics

High Availability Reference Information, on page 908
How to Configure HA Between the Primary and Secondary Servers, on page 884

Remove HA During Restore

Cisco EPN Manager does not back up configuration settings related to high availability. If you are restoring an implementation that is using HA, you should only restore data to the primary server. The restored primary server will automatically replicate its data to the secondary server. If you try to run a restore on a secondary server, Cisco EPN Manager generates an error message.

Follow these steps when restoring an implementation that uses HA:

1. Use the GUI to remove the HA settings from the primary server. See Remove HA Via the GUI, on page 912.
2. Restore data on the primary server. See Restore Cisco EPN Manager Data, on page 746.
3. When the restore process is complete, perform the HA configuration process again. See How to Configure HA Between the Primary and Secondary Servers, on page 884.

Reset the Server IP Address or Host Name

Avoid changing the IP address or hostname of the primary or secondary server, if possible. If you must change the IP address or hostname, remove the HA configuration from the primary server before making the change. When finished, re-register HA.

Resolve TOFU Failure at Any State

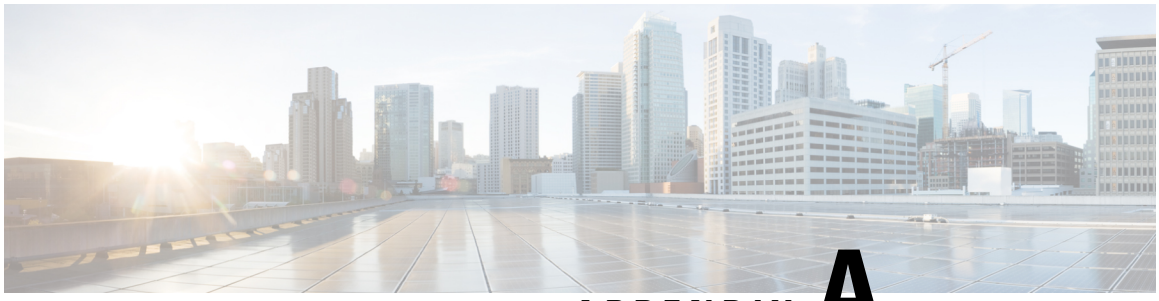
When the primary and secondary servers communicate, there is a possibility of a TOFU error as mentioned below.

You must correct the following error(s) before proceeding. 'A Trust-on-first-use (TOFU) based Certificate is configured for this connection. The current certificate on the remote host is different than what was used earlier.

To resolve this issue:

- Clear the existing certificate using the NCS CLI command on both the primary and secondary servers.

```
ncs certvalidation tofu-certs deletecert host <server-hostname>
```



APPENDIX A

Best Practices: Harden Your Cisco EPN Manager Security

Security hardening entails making adjustments to ensure that the following components optimize their security mechanisms:

- Cisco EPN Manager web server
- Cisco EPN Manager server
- Cisco EPN Manager storage system (local or external)
- Communication between Cisco EPN Manager and devices
- User authentication system (local or external)
- Time synchronizing system that use Network Time Protocol (NTP)

This appendix will first cover a few core security concepts that administrators should know about. It will then cover the specific tasks that need to be completed in order to optimize Cisco EPN Manager security.

Core Security Concepts

If you are an administrator and are looking to optimize the security of your Cisco EPN Manager product, you should have a good understanding of the following security concepts.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) or its subsequent standardization, Transport Layer Security (TLS), to encrypt the data transmitted over a channel. Several vulnerabilities have been found in SSL, so Cisco EPN Manager now supports TLS only.

Note TLS is loosely referred to as SSL often, so we will also follow this convention.

SSL employs a mix of privacy, authentication, and data integrity to secure the transmission of data between a client and a server. To enable these security mechanisms, SSL relies upon certificates, private-public key exchange pairs, and Diffie-Hellman key agreement parameters.

Note Device database backup fails if the device uses TLS version less than 1.2 for HTTPSS communication. For example, NCS2000/ONS 10.5 version.

SSL Certificates

SSL certificates and private-public key pairs are a form of digital identification for user authentication and the verification of a communication partner's identity. Certificate Authorities (CAs), such as VeriSign and Thawte, issue certificates to identify an entity (either a server or a client). A client or server certificate includes the name of the issuing authority and digital signature, the serial number, the name of the client or server that the certificate was issued for, the public key, and the certificate's expiration date. A CA uses one or more signing certificates to create SSL certificates. Each signing certificate has a matching private key that is used to create the CA signature. The CA makes signed certificates (with the public key embedded) readily available, enabling anyone to use them to verify that an SSL certificate was actually signed by a specific CA.

In general, setting up certificates in both High Availability (HA) and non-HA environments involves the following steps:

1. Generating an identity certificate for a server.
2. Installing the identity certificate on the server.
3. Installing the corresponding root certificate on your client or browser.

The specific tasks you need to complete will vary depending on your environment.

Note the following:

- The start-stop sequencing of servers needs to be done carefully in HA environments.
- Non-HA environments, where a virtual IP address is configured, require the completion of a more complicated certificate request process.

1-Way SSL Authentication

This authentication method is used when a client needs assurance that it is connecting to the right server (and not an intermediary server), making it suitable for public resources like online banking websites. Authentication begins when a client requests access to a resource on a server. The server on which the resource resides then sends its server certificate (also known as an SSL certificate) to the client in order to verify its identity. The client then verifies the server certificate against another trusted object: a server root certificate, which must be installed on the client or browser. After the server has been verified, an encrypted (and therefore secure) communication channel is established. At this point, the Cisco EPN Manager server prompts for the entry of a valid username and password in an HTML form. Entering user credentials after an SSL connection is

established protects them from being intercepted by an unauthorized party. Finally, after the username and password have been accepted, access is granted to the resource residing on the server.

Note A client might need to store multiple server certificates to enable interaction with multiple servers.

To determine whether you need to install a root certificate on your client, look for a lock icon in your browser's URL field. If you see this icon, this generally indicates that the necessary root certificate has already been installed. This is usually the case for server certificates signed by one of the bigger Certifying Authorities (CAs), because root certificates from these CAs are included with popular browsers.

If your client does not recognize the CA that signed a server certificate, it will indicate that the connection is not secure. This is not necessarily a bad thing. It just indicates that the identity of the server that you want to connect has not been verified. You can install the necessary root certificate on your client or browser. A lock icon in your browser's URL field indicates the certificate was installed successfully.

Cisco EPN Manager Security Hardening Overview

Hardening Cisco EPN Manager security requires completion of the following tasks:

(During installation)

- Configuring HTTPS and setting up 1-way SSL authentication for standalone servers and HA environments
- Shutting down insecure and unused ports
- Configuring network firewalls
- Configuring external authentication

(Post installation)

- Updating certificates in response to changes (like setting a new hostname or IP address)
- Hardening the Cisco EPN Manager server, as needed

Harden the Cisco EPN Manager Web Server

To harden the Cisco EPN Manager web server, do the following:

1. Make Web Server Connectivity Secure By Using HTTPS, on page 918
2. Set Up Certificate-Based Authentication for Web Clients, on page 918
3. Configure a Custom OCSP Responder on the Server, on page 920

Make Web Server Connectivity Secure By Using HTTPS

The Cisco EPN Manager web server should be configured to use HTTPS instead of HTTP. This protects the systems that connect to the web server and also avoids the possibility of any client indirectly intruding into the web server and other participating systems. HTTPS requires using a Certificate Authority (CA) certificate in the web server and appropriate SSL mechanisms.

Set Up Certificate-Based Authentication for Web Clients

For higher-level security, the Cisco EPN Manager server should authenticate clients by using certificate-based authentication. With this form of authentication, Cisco EPN Manager first validates the client's associated certificate to ensure that the client is authentic and then it validates the username and password. This mechanism prevents unauthorized machines (that is, machines for which no certificate exists) to connect with the web server. Cisco EPN Manager implements this feature using the Online Certificate Status Protocol (OCSP).

Note The certificate(s) discussed in this topic uniquely identify the *clients*. This is different from the certificate for the *web server*, which was used to set up HTTPS operation. While this procedure is similar to the procedure for generating CER files for web server certificates, it is not exactly the same. You might need to use other tools (such as OpenSSL). In addition, there are different methods for generating CA certificate files. If you need assistance, contact your Cisco representative.

To configure certificate-based authentication:

Step 1 Generate the client certificate files using a CA, which normally involves the following steps:

a) Generate the public key.
b) Generate the CSR file containing the public key.
c) Submit the CSR file to a CA to get the certificate file(s).
d) If you receive multiple files, do not concatenate the files to make a single CER/PEM file. Instead:

- Give the *Client* certificate file to the application user to keep in the client machine.
- Keep the *Root* and all *Intermediate* CA certificates. You will import them into the server in Step 4.

Note You should get these certificates from the root and intermediate CA servers. Do not use any files received from a non-trusted source.

Note Do not import the Client CA certificate into the web server. Keep that file with the client machine—for example, on an insertable card, a hardware or software token device, and so forth. When the client browser tries to connect to the Cisco EPN Manager web server, the web server instructs the client browser to ask for the Client certificate. The user must provide the Client certificate, and then enter their username and password.

Step 2 Log in to the Cisco EPN Manager server using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server, on page 765. Do not enter config mode.

Step 3 Import the Root CA and Intermediate CA certificate files, one at a time, into the Cisco EPN Manager web server.

a) Import the Root CA certificate file with this command:

```
ncs key importcacert aliasName rootCACertFile repository repoName
```

Where:

- *aliasName* is the short name supplied for the CA certificate.
- *rootCACertFile* is the Root CA certificate filename.
- *repoName* is the location of the Cisco EPN Manager repository where the certificate file is hosted.

Note Note that this command is very different from the command used to apply the server certificate.

b) Import the Intermediate CA certificate file with this command:

```
ncs key importcacert aliasName intermediateCACertFile repository repoName
```

Where:

- *intermediateCACertFile* is the Intermediate CA certificate filename.

Step 4 Restart the server(s). The procedure you should follow depends on whether your deployment is configured for high availability.

For deployments *without* high availability, restart the Cisco EPN Manager server to apply the changes.

```
ncs stop
ncs start
```

For deployments *with* high availability, follow these steps, being sure to restart the servers in the correct order.

a) On the *secondary* server, log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

Note Do not restart the secondary server until you reach Step 5(e).

b) Verify that the secondary server is stopped.

c) On the *primary* server, log in as the Cisco EPN Manager CLI admin user and stop the server:

```
ncs stop
```

Note Do not restart the primary server until you reach Step 5(f).

d) Verify that the primary server is stopped.

e) On the *secondary* server, run the following commands:

1. Run the **ncs start** command to restart the server.
2. Verify that the secondary server has restarted.
3. Run the **ncs status** command and verify that the Health Monitor process is running.
4. Run the **ncs ha status** command and verify that the HA status of the secondary server is **Secondary Lost Primary**.

f) On the *primary* server, run the following commands:

1. Run the **ncs start** command to restart the server.
2. Verify that the primary server has restarted.
3. Run the **ncs status** command and make sure that the Health Monitor process and other processes have restarted.

Once all the processes on the primary server are up and running, HA registration is automatically triggered between the secondary and primary servers (and an email is sent to the registered email addresses). This normally completes after a few minutes.

g) Verify the HA status on the primary and secondary servers by running the **ncs ha status** command on both servers. You should see the following :

- The primary server state is **Primary Active**.
- The secondary server state is **Secondary Syncing**.

Configure and Manage OCSP on the Server

Online Certificate Status Protocol (OCSP) enables certificate-based authentication for web clients using OCSP responders. Typically, the OCSP responder URL is read from the certificate's Authority Information Access (AIA). As a failover mechanism, configure the OCSP responder URL on the Cisco EPN Manager server.

Configure a Custom OCSP Responder on the Server

To configure a custom OCSP responder URL on the Cisco EPN Manager server:

Step 1 Log in to the Cisco EPN Manager server using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server, on page 765. Do not enter config mode.

Step 2 (Optional) You can enter the following command to check what is configured on the server:

```
show security-status
```

Step 3 Enter the following command to enable client certificate authentication:

```
ncs run client-auth enable
```

Step 4 Enter the following command to enable the custom OCSP responder URL to override a value of the OCSP responder URL in the certificate.

```
ncs certvalidation custom-ocsp-responder enable
```

Step 5 Enter the following command to set the custom OCSP responder URL:

```
ncs certvalidation custom-ocsp-responder set url1 responderURL
```

Where:

- *responderURL* is the URL of the OCSP responder, as taken from the client CA certificate.

Delete a Custom OCSP Responder from the Server

To delete an existing custom OCSP responder defined on the Cisco EPN Manager server:

Step 1 Execute the **show security-status** command to view the custom OCSP responders that are currently configured on the server, and identify the number of the responder you want to delete.

Step 2 Delete the OCSP responder from the server:

```
ncs certvalidation custom-ocsp-responder clear url1
```

Harden the Cisco EPN Manager Server

Follow these steps to harden the Cisco EPN Manager server.

1. Disable Insecure Ports and Services, on page 921
2. Use SNMPv3 to Harden Communication Between Cisco EPN Manager and Devices, on page 720
3. Set Up External Authentication Using the CLI, on page 720
4. Disable Accounts Not Needed for Day-to-Day Operations, on page 922
5. Harden NTP, on page 723

Disable Insecure Ports and Services

As a general policy, any ports that are not needed and are not secure should be disabled. You need to first know which ports are enabled, and then decide which of these ports can be safely disabled without disrupting the normal functioning of Cisco EPN Manager for your deployment. You can do this by listing the ports that are open and comparing it with a list of ports that are safe to disable.

You can get this list of ports which are safe to disable from Cisco Evolved Programmable Network Manager Installation Guide,which lists the ports and services used by Cisco EPN Manager.

Follow the procedure below to find out which ports are enabled.

Step 1 Log in to Cisco EPN Manager using the command line, as explained in Establish an SSH Session With the Cisco EPN Manager Server, on page 765. Do not enter config mode.

Step 2 The show security-status command displays the server's currently open (enabled) TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. You will see output similar to the following:

```
show security-status
Open TCP Ports       22 443 1522 8082
Open UDP Ports       162 514 9991
FIPS Mode            enabled
TFTP Service         disabled
FTP Service          disabled
JMS port (61617)     disabled
Root Access          disabled
Client Auth          enabled
OCSP Responder1      http://209.165.200.224/ocsp
OCSP Responder2      http://209.165.202.128/ocsp
```

Step 3 Check the Cisco Evolved Programmable Network Manager Installation Guide for the table of ports used by Cisco EPN Manager, and see if your ports are listed in that table. That table will help you understand which services are using the ports, and which services you do not need—and thus can be safely disabled. In this case, *safe* means you can *safely disable the port without any adverse effects to the product* .

Note If you are not sure whether you should disable a port or service, contact your Cisco representative.

Step 4 Disable the insecure ports using the Cisco EPN Manager GUI.

This example disables FTP and TFTP, which are not secure protocols and should be disabled (use SFTP or SCP instead). TFTP and FTP are typically used to transfer firmware or software images to and from network devices and Cisco EPN Manager.

a) Log in to Cisco EPN Manager with a user ID that has Administrator privileges.
b) Choose **Administration** > **Settings** > **System Settings**, then choose **General** > **Server**.
c) Under **FTP** and **TFTP**, select **Disable**, then click **Save**.
d) Restart Cisco EPN Manager. See Stop and Restart Cisco EPN Manager, on page 769.

Note In High Availability setup, ensure you disable FTP and TFTP services on the secondary server before configuring High Availability. See Enable FTP/TFTP/SFTP Service on the Server, on page 767 for more information.

Step 5 Create a new ACL and attach to desired interface. See Create or Modify an IP Access-List to Filter Network Traffic , on page 775.

Step 6 If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco EPN Manager to operate. For more information, refer to the Cisco Evolved Programmable Network Manager Installation Guide (specifically, the information about ports that are used by Cisco EPN Manager and suggested firewall configurations). If you need further help, contact your Cisco representative.

Disable Accounts Not Needed for Day-to-Day Operations

The Cisco EPN Manager web GUI root user should be disabled after creating at least one other web GUI user that has root privileges. See Disable and Enable the Web GUI root User, on page 792.

Harden Your Cisco EPN Manager Storage

We recommend that you secure all storage elements that will participate in your Cisco EPN Manager installation, such as the database, backup servers, and so on.

Contact your Cisco representative for more information about hardening your internal or external storage. In the case of external storage, also contact your storage vendor.

If you ever uninstall or remove Cisco EPN Manager, make sure that all VM-related files that might contain sensitive data are digitally shredded (as opposed to simply deleted).

Harden NFS-Based Storage

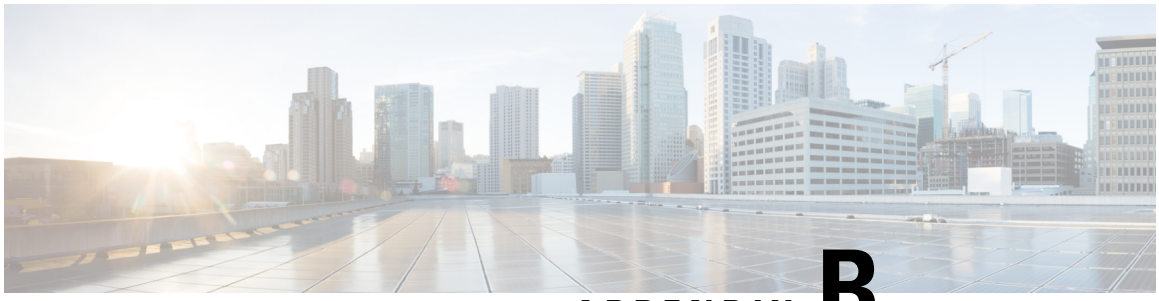
Since NFS does not have built-in security, you must implement as many of the following security measures as possible to secure the NFS server:

- Set up a firewall in front of the NFS server—To do this practically, tie down the ports that NFS will use in various configuration files and then specify those ports in the firewall configurations.
- Use a port mapper—On the NFS server, only allow NFS transactions that involve specific IP addresses.
- To prevent attacks via a compromised DNS, only specify IP addresses (and not domain names) when configuring NFS.
- When setting up the export of folders, use the **root_squash** option in the /etc/exports file.
- When configuring the /etc/exports file, use the **secure** option.
- When configuring the backup staging and storage folders, use the **nosuid** and **noexec** mount options.

Note It is not mandatory to configure a staging folder.

- For the storage folder (and optional staging folder), configure a file access permission value of **755** (which grants all users read and write privileges) and set userid **65534** (the user **nobody**, who does not have any system privileges) as the owner.
- Tunnel NFS traffic either through SSH or SSL/TLS. For SSH, use RSA key-based authentication instead of user authentication.

Do not rely on just one of these measures to secure your NFS-based storage. Your best bet is to implement the combination of measures that best suits your situation. Also keep in mind that this list is not an exhaustive one. To achieve a higher level of confidence when hardening your storage, we recommend that you discuss your situation with a Linux system admin and a security expert beforehand.



APPENDIX B

Icon and State Reference

Device Reachability and Admin States

Device Reachability State—Indicates whether Cisco EPN Manager can communicate with the device using all configured protocols.

Table 64: Device Reachability State

Icon	Device Reachability State	Description	Troubleshooting
	Reachable	Cisco EPN Manager can reach the device using SNMP, or the NCS 2K device using ICMP.	—
	Ping reachable	Cisco EPN Manager can reach the device using Ping, but not via SNMP.	Although ICMP ping is successful, check for all possible reasons why SNMP communication is failing. Check that device SNMP credentials are the same in both the device and in Cisco EPN Manager, whether SNMP is enabled on the device, or whether the transport network is dropping SNMP packets due to reasons such as mis-configuration, etc. See Change Basic Device Properties, on page 315.

	Unreachable	Cisco EPN Manager cannot reach the device using Ping.	Verify that the physical device is operational and connected to the network.
	Unknown	Cisco EPN Manager cannot connect to the device.	Check the device.

Device Admin State—Indicates the configured state of the device (for example, if an administrator has manually shut down a device, as opposed to a device being down because it is not reachable by Ping).

Table 65: Device Admin State

Device Admin State	Description	Troubleshooting
Managed	Cisco EPN Manager is actively monitoring the device.	Not Applicable.
Maintenance	Cisco EPN Manager is checking the device for reachability but is not processing traps, syslogs, or TL1 messages.	To move a device back to Managed state, see Move a Device To and From Maintenance State, on page 68.
Unmanaged	Cisco EPN Manager is not monitoring the device.	In the Network Devices table, locate the device and click the "i" icon next to the data in the **Last Inventory Collection Status** column. The popup window will provide details and troubleshooting tips. Typical reasons for collection problems are: • Device SNMP credentials are incorrect. • The Cisco EPN Manager deployment has exceeded the number of devices allowed by its license. • A device is enabled for switch path tracing only. If a device type is not supported, its Device Type will be **Unknown**. You can check if support for that device type is available from Cisco.com by choosing **Administration** > **Licenses and Software Updates** > **Software Update** and then clicking **Check for Updates**.
Unknown	Cisco EPN Manager cannot connect to the device.	Check the device.

Device Sync State

Device Sync State—Indicates status of the Sync operation performed on a device.

Table 66: Device Sync State

Icon	Device Sync State	Description
	Synchronizing	Device synchronization is in progress.
	Completed	Device synchronization completed successfully.
	Error/Warning	List of errors or warnings indicated: • Add Initiated • Collection Failure • Completed with Warning • Delete In Progress • In Service • In Service Maintenance • No License • Partial Collection Failure • SNMP Connectivity Failed • SNMP User Authentication Failed • Switch Port Trace • Wrong CLI Credentials

Note In Service Maintenance filter is not available for Last inventory collection status.

Port or Interface States

Port or Interface Primary States—Conveys the most important state information for a port or interface by combining the admin and operational states. The Multilayer Trace displays either a port's primary state or alarm status. For the Chassis View, if an element does not support the changing of color to indicate a state change, you can still get the state change information from the alarm that is generated.

Note If there is an alarm associated with a port/interface, alarm icon will show up, port icon will not show. The alarm is shown only in case the port is not in test or admin down state.

Port or Interface Primary State	Icon	Admin Status	Operational State

Unknown		Unknown	Unknown
Down		Up	Down
Testing		Test	—
Admin Down		Admin Down	—
Up		Up	Up
Auto Up		Up	Auto Up

Port or Interface Admin Status—Represents the configured state of the port or interface (for example, if an administrator has manually shut down a port).

Port or Interface Admin Status	Icon	Description
Unknown		Port or interface admin status is unknown. There is no response (or insufficient response) from the device.
Admin Down		Port or interface was manually shut down by the administrator.
Up		Port or interface is enabled by the administrator.
Testing		Port or interface is being tested by the administrator.

Port or Interface Operational State—Conveys the port or interface's running state and whether it is working properly.

Port or Interface Operational State	Icon	Description
Unknown		Port or interface operational state is unknown. There is no response (or insufficient response) from the device.
Down		Port or interface is not working properly.
Up		Port or interface is receiving and transmitting data.
Auto Up		Port or interface is receiving and transmitting data (only certain devices support this state; other devices use "Up").

Circuit or VC States

Circuit or VC Primary States— Conveys the most important state information for a circuit, in this order: Serviceability, Discovery, Alarm, Provisioning. It is normally shown in the first column of a circuit or VC table.

Circuit or VC Primary State	Icon	Serviceability	Discovery	Alarm	Provisioning
Missing		—	Missing	—	—
Down		Down	—	—	—
Critical		—	—	Critical	—
Major		—	—	Major	—
Minor		—	—	Minor	—
Partially Down		Partial	—	—	—
Admin Down		Admin Down	—	—	—
Partially Discovered		—	Partial	—	—
Failed		—	—	—	(Create, modify, or delete) failed
In progress		—	—	—	(Create, modify, or delete) in progress
Warning			—	Warning	—
Up		Up	—	—	—
Auto Up		Auto Up	—	—	—
Info		—	—	Info	—
Cleared		—	—	Cleared	—

Circuit or VC Serviceability State— This value is a combination of the circuit or VC's admin and operational states. The admin state is shown because it impacts service operability. For optical circuits, the admin state also determines whether the Activate and Deactivate actions are available. The operational state is shown to quickly identify whether a service is working or not.

Circuit or VC Serviceability State	Icon	Description
Admin Down		Circuit or VC manually shut down by the administrator.
Down		Circuit or VC is operationally down and administratively up.
Up		Circuit or VC is operationally and administratively up.

Auto Up		Circuit or VC is operationally auto up and administratively up. Only certain devices support the Auto Up operational state.
Unavailable		Circuit or VC has not been discovered yet, or its operational status is unavailable.
Partial		Circuit/VC operational or administrative state is partial. • Partial admin state—The circuit or VC has a mixed administrative request (to activate some service resources and deactivate others), has a mix of resources that are administratively up and down, or has resources whose operational state is unavailable. • Partial operational state—The circuit or VC has a mix of some active and deactivated resources, or the operational state for some of its resources are unavailable.
Up - Unprotected		The circuit/VC that was configured with a protection path is operational but cannot switch to the alternate path because of severe failures. **Note** This serviceability status indication is supported for OCHCC WSON circuits with Y-Cable protection and protected ODU.

Following table provides details of the serviceability states of Circuits/VCs under various scenarios:

Technology	Service Type	Scenario	Serviceability State

Carrier Ethernet	EPL, EVPL, Access EPL, and Access EVPL	If the operational state of the endpoints (service instance / subinterface), cross connects, and pseudowire participating in the service is up	Up
		If the admin state of both the source and destination endpoints (service instance / subinterface) participating in the service is down	Admin Down
		In all the other scenarios, when at least one endpoint (service instance / subinterface), cross connect, or the pseudowire participating in the service is down	Down
	EP-LAN, EVP-LAN, EP-Tree, and EVP-Tree	If all the endpoints (service instance / subinterface), bridge domains, VFIs, and pseudowires participating in the service are up	Up
		If the operational state of at least two endpoints (service instance / subinterface) participating in the service are up and the rest of the endpoints are down	Partial
		If the admin state of all the endpoints (service instance / subinterface) participating in the service is down	Admin Down
		If the operational state of at least one endpoint (service instance / subinterface) participating in the service is up and the rest of the endpoints are down	Down

Icon and State Reference

Circuit Emulation	All service types	If the operational state of the endpoints (cemGroup), underlying TDM controller, cross connect, and pseudowire participating in the service are up	Up
		If the admin state of both the source and destination endpoints (cemGroup) participating in the service is down	Admin Down
		In all the other scenarios, when the operational state of one of the endpoints (cemGroup), underlying TDM controller, cross connect, and pseudowire participating in the service is down	Down
MPLS	Unidirectional TE Tunnel	If the operational state of the tunnel interface is up	Up
		If the admin state of the tunnel interface is down	Admin Down
		In all the other scenarios, when the operational state of the tunnel is down	Down
	Bidirectional TE Tunnel	If the operational states of the interfaces on both ends of the tunnel is up	Up
		If the admin states of the interfaces on both ends of the tunnel is down	Admin Down
		In all the other cases, when the operational state of the tunnel interface is down	Down

Serial	RS232, RS422, and RS485	If the operational state of the endpoints (channelGroup), underlying Serial interface, cross connect, and pseudowire participating in the service are up	Up
		If the admin state of both the source and destination endpoints (channelGroup) participating in the service is down If the admin state of either source or destination endpoint (channelGroup) is down	Admin Down
		In all the other scenarios, when the operational state of one of the endpoints (channelGoup), underlying Serial interface, cross connect, and pseudowire participating in the service is down	Down
	Raw Socket	If server and all its associated client sessions are up	Up
		If server is up and all its associated client sessions are down	Down
		If the admin state of both the source and destination endpoints (channelGroup) participating in the service is down If the admin state of a server or admin state of all the participating clients are down	Admin Down
		If server and all its associated client sessions are down	Down

		If server is up and if any one of its associated clients is up	Partial
Layer 3 VPN		If the operational state of all the endpoints (subinterface, BDI, and BVI) participating in the service is up	Up
		If the operational state of at least two endpoints (subinterface, BDI, and BVI) participating in the service are up and the rest of the endpoints are down	Partial
		If the admin state of all the endpoints (subinterface, BDI, and BVI) participating in the service is down	Admin Down
		If the operational state of at least one endpoint (subinterface, BDI, and BVI) participating in the service is up and the rest of the endpoints are down.	Down
SR TE	SR Policy	If the operational state of the SR policy us up	Up
		If the admin state of the SR policy is down	Admin Down
		In all the other scenarios, if the operational state of the SR policy is down	Down

Circuit or VC Discovery State—Represents the latest state and structure of a service and its components, as discovered from the network. Having a Discovered version means that the application is actually monitoring the service itself, e.g. it can define meaningful operational and performance data.

Circuit or VC Discovery State	Icon	Description
Partial		Circuit or VC partially discovered by Cisco EPN Manager; not all of its expected entities have been discovered.

Full		Circuit or VC fully discovered by Cisco EPN Manager, so that the Cisco EPN Manager can monitor the service and provide meaningful operational and performance data.
Missing		Circuit or VC not yet discovered by Cisco EPN Manager (though it may have been provisioned).
Resync		Circuit or VC is resynced.

Circuit or VC Provisioning State—Represents whether there is a provisioning intent for a circuit or VC and, if so, its status. If a reconciliation report has been generated, the state of the reconcile action is reflected.

Circuit or VC Provisioning State	Icon	Description
None		Circuit or VC was discovered but has not yet been provisioned. The circuit/VC must be promoted in order to modify or delete it.
Failed		Action has failed.
In Progress		Action was initiated but not yet completed.
Planned		Action is planned but not yet initiated.
Succeeded		Action has completed successfully.

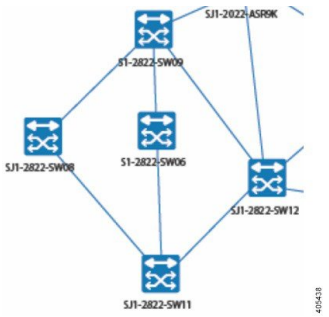
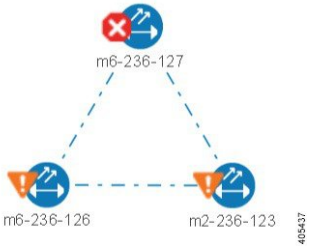
Link Serviceability States

Serviceability State	Icon	Description
Admin Down		Link was purposefully shut down by the administrator.
Down		Link is down (but it should not be).
Up		Link is up and traffic is passing through the link.
Auto Up		Link is up because it detected a signal (this state is only supported by optical devices).
Unavailable		Link is not discovered yet or its status is unavailable.

Partial		Link has a mismatch between requests, resources, or resource states. Examples: • Link is processing a request to activate some service resources and deactivate others. • Link has some active and some deactivated resources. • Some link resources are up and others are down. • The state for one of the link's resources is not known.

Link Characteristics

The following table describes the different types of links used to represent the connection between devices in the Topology Map view of Cisco EPN Manager.

Link Type	Description
	Solid Line-—Indicates a physical, topological, or service link, such as a link between two devices.
	Dashed Line—Indicates an association or business link between elements such as EVCs, VPLS service instances, or VPN components.

Equipment Operational States (Chassis View)

The equipment operational states represent the running state of the network element.

Equipment Operational State	Icon	Description
In Service	(none)	Equipment is operating properly.

Pre-provisioned		(Cisco NCS 2000 and Cisco ONS devices only) Equipment has been configured but is not physical present in the chassis.
Failed/Disabled/Down/Out of Service/Out of Service Maintenance		Equipment is not operating properly.
Unknown		Equipment operational state is unknown. No response (or insufficient response) from the device.

Alarm Severity Icons

The table below lists the alarm colors and their respective severity levels for the icons displayed in various parts of the web GUI.

Severity Icon	Description	Color
	Critical alarm	Red
	Major alarm	Orange
	Minor alarm	Yellow
	Warning alarm	Light Blue
	Alarm cleared; normal, OK	Green
	Informational alarm	Medium Blue
	Indeterminate alarm	Dark Blue

Device Type Icons

Table below defines the icons used to represent different device types in the Topology and the Multi-layer Trace views in Cisco EPN Manager.

Icon	Definition
	Switch

Icon and State Reference

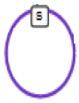
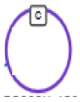
Icon	Definition
	Router
	Router Aggregated
	Cisco NCS 6000 device on which a Secure Domain Router (SDR) resides. The SDR's name is listed directly above the device's icon. **Note** There may be cases where the SDR label for a device that belongs to a cluster or user-defined group is not displayed (since auto-clustering is applied to devices based on their proximity).
	Router configured with an L3VPN service.
	Switch Aggregated
	Access Point
	Service Module
	UCS C-Series
	NAM Blade

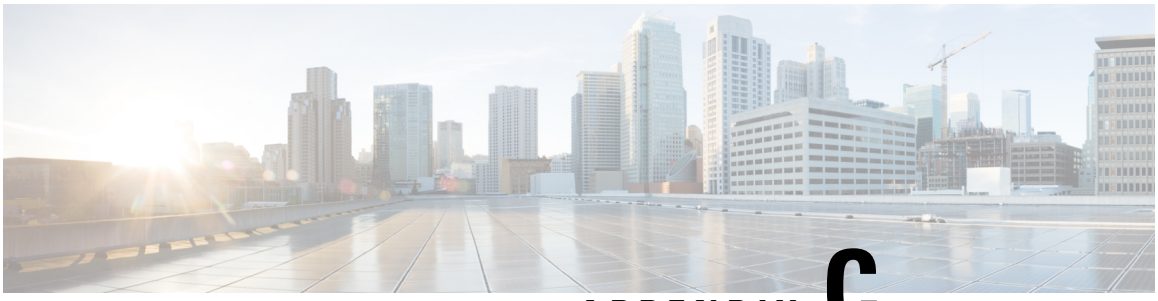
Icon	Definition
	Group
	Generic Device
	Virtual Server
	Wireless LAN Controller
	Unknown
	DWDM ROADM Regeneration/NCS 2000

Circuit or VC Network Topology Overlay Icons

Overlay Icon	Definition
	Source endpoint
	Destination endpoint
	EVC or CEM service with local switching

Icon and State Reference

Overlay Icon	Definition
	Endpoint included by the user during creation o **Note** "S" appears for both adjacent and n
	Endpoint excluded by the user during the creati
	Endpoint with some ports that were either inclu routes of the circuit.
	E-TREE EVC endpoint that has been designate
	S on the icon represents that the server is config
	C on the icon represents that the client is config
	S and C on the icon represents that both server a
	Selected endpoint.
	Hub; If the hub and root are on the same device
	Link included during creation of the circuit.
	Link excluded during creation of the circuit.
	Endpoint with some ports that were either inclu participating in various routes of the same circu



APPENDIX C

Cisco EPM Notification MIB

CISCO-EPM-NOTIFICATION-MIB

This appendix contains the CISCO-EPM-NOTIFICATION-MIB.

SNMP Varbind	Data Type	Varbind OID	SNMP Varbing Description	Example
cenAlarmVersion	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.2	The release version of this MIB.	1.0
cenAlarmTimestamp	Timestamp	.1.3.6.1.4.9.9.311.1.1.2.1.3	The time when the alarm was raised. **Note** This is the number of seconds since Jan 1st 1970 (since epoch) in UTC.	1523608787
cenAlarmUpdatedTimestamp	Timestamp	.1.3.6.1.4.9.9.311.1.1.2.1.4	Alarms persist over time and its value is updated automatically when the field(s) is changed. The updated time denotes a time. Each alarm is identified by the unique alarm instance id, For example, cenAlarmInstanceID.	1523608788
cenAlarmInstanceID	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.5	The Unique Alarm Instance ID.	1185098114
cenAlarmStatus	Integer	.1.3.6.1.4.9.9.311.1.1.2.1.6	The alarm status indicates the status of the alarm in integer value.	Active=2, Cleared=3
cenAlarmStatusDefinition	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.7	The short description of the status of the alarm. The string is formatted in ',' tuples. The value is the same value that the 'cenAlarmStatus'attribute holds. Contains one line description of the alarm status generated.	2, ACTIVE3, CLEARED

SNMP Varbind	Data Type	Varbind OID	SNMP Varbing Description	Example
cenAlarmType	Integer	.1.3.6.1.4.9.9.311.1.1.2.1.8	• unknown(1) —When the value for this attribute could not be determined. • direct(2)— Denotes an alarm generated by a set of events where all events are reported by an observation(s) of a managed object. • indirect(3)—Denotes an alarm generated by a set of events where all events were deduced or inferred by the status of managed objects as determined by the network management system. • mixed(4)—Denotes an alarm generated by a set of events which were either direct or indirect.	2
cenAlarmCategory	Integer	.1.3.6.1.4.9.9.311.1.1.2.1.9	The category of the alarm generated represented in integer value. **Note** This integer field is not used in EPN Manager. Use cenAlarmCategoryDefinition instead, which is a string.	—
cenAlarmCategoryDefinition	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.10	The short description of the category of the alarm generated. The String is formatted in ',' tuples. The value is the same value that the 'cenAlarmCategory' attribute holds. Contains one line description of the alarm category generated. For a list of alarm types, see the 'Alarm Name column in the following documents. These are for 2.1 (Derecho). For other versions, use cisco.com published documentation for the version that you need. Cisco Evolved Programmable Network Manager Supported SNMP Traps Cisco Evolved Programmable Network Manager Supported Syslogs Cisco Evolved Programmable Network Manager Supported TL1 Messages Cisco Evolved Programmable Network Manager Supported Alarms	"LINK_DOWN", "SWT_AUTH_FAIL", "LINK_UP"

SNMP Varbind	Data Type	Varbind OID	SNMP Varbing Description	Example
cenAlarmServerAddressType	InetAddressType	.1.3.6.1.4.9.9.311.1.1.2.1.11	The type of Internet address by which the server is reachable. The server is the server that is generating this trap.	0: unknown 1:ipv4 2:ipv6
cenAlarmServerAddress	InetAddress	.1.3.6.1.4.9.9.311.1.1.2.1.12	The IP Address or the DNS name of the Management. Server that raised this alarm will be notified.	10.127.101.145
cenAlarmManagedObjectClass	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.13	The class of the managed object for which this alarm was generated. For example, Router, Switch, GateKeeper, and VoicePort. For a list of categories, see the 'Category' column in the following documents. These are for 2.1 (Derecho). For other versions, use cisco.com published documentation for the version that you need. Cisco Evolved Programmable Network Manager Supported SNMP Traps Cisco Evolved Programmable Network Manager Supported Syslogs Cisco Evolved Programmable Network Manager Supported TL1 Messages Cisco Evolved Programmable Network Manager Supported Alarms	"Optical", "Carrier Ethernet"
cenAlarmManagedObjectAddressType	InetAddressType	.1.3.6.1.4.9.9.311.1.1.2.1.14	The type of Internet address by which the managed object is reachable.	0: unknown 1: ipv4 2: ipv6
cenAlarmManagedObjectAddress	InetAddress	.1.3.6.1.4.9.9.311.1.1.2.1.15	The IP Address or the DNS name of the Managed Object.	2405:200:204:138:172:30:9.121

SNMP Varbind	Data Type	Varbind OID	SNMP Varbing Description	Example
cenAlarmDescription	OctetString	.1.3.6.1.4.1.9.9.311.1.1.2.1.16	A detailed description of the alarm. For a list of alarm descriptions, see the 'Description/Probable Cause' column in the following documents. These are for 2.1 (Derecho). For other versions, use cisco.com published documentation for the version that you need. Cisco Evolved Programmable Network Manager Supported SNMP Traps Cisco Evolved Programmable Network Manager Supported Syslogs Cisco Evolved Programmable Network Manager Supported TL1 Messages Cisco Evolved Programmable Network Manager Supported Alarms	Port 'GigabitEthernet0/0/6' (Description: ' # TO GigabitEthernet0/0/7 #') is down on device [illegible] Carrier
cenAlarmSeverity	Integer	.1.3.6.1.4.1.9.9.311.1.1.2.1.17	The alarm severity indicates the severity of the alarm in integer value. • 0—Critical • 1—Major • 2—Minor • 3—Warning • 4—Clear • 5—Info	4

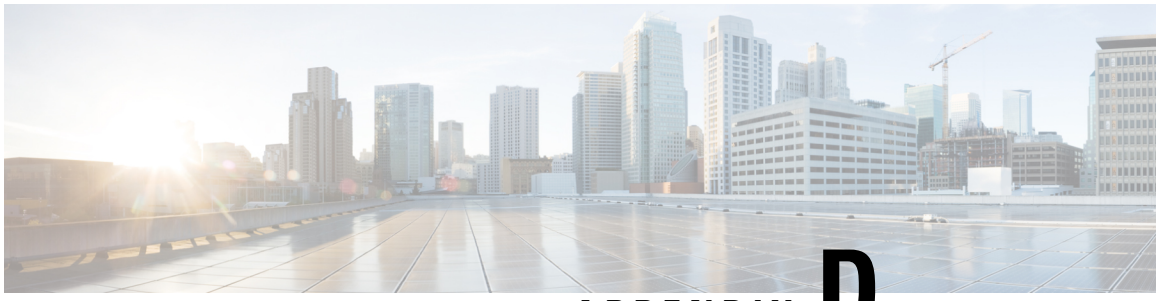
SNMP Varbind	Data Type	Varbind OID	SNMP Varbing Description	Example
cenAlarmSeverityDefinition	SnmpAdminString	.1.3.6.1.4.1.9.9.311.1.1.2.1.18	The short description of the severity of the alarm generated. The String is formatted in ',' tuples. The value is the same value that the 'cenAlarmSeverity ' attribute holds. Contains one line description of the alarm severity generated. • 0—Critical • 1—Major • 2—Minor • 3—Warning • 4—Clear • 5—Info	4.CLEARED
cenAlarmTriageValue	Integer	.1.3.6.1.4.1.9.9.311.1.1.2.1.19	The triage value of an alarm is a hierarchical weighting value (applied by the application, and more importantly customizable by the end user) to allow an artificial form of evaluating impact, interest, or other user-determined functions between alarms. The value is a positive number or zero, which denotes an undetermined or uncomputable value. **Note** EPN manager does not support this field.	—
cenEventIDList	OctetString	.1.3.6.1.4.1.9.9.311.1.1.2.1.20	Comma separated list of the Unique Event identifiers that led to the generation of this Alarm. **Note** EPN manager does not support this field.	—

SNMP Varbind	Data Type	Varbind OID	SNMP Varbing Description	Example
cenUserMessage1	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.21	User input message. Information about the alarm including whether the alarm is a root cause alarm or a service - impacting alarm. srcObjectDisplayName=GigabitEthernet0/0/0/18, rootCauseId=0, hostName=ASR9001-156.156.cisco, serviceImpacting=0, applicationSpecificAlarmID=LINK_DOWN:10.127.101.156:If: GigabitEthernet0/0/0/18##SubAlarm@@_7, correlationType=UNKNOWN, srcObjectBusinessKey=4c2b8aa7[1589721133_10.127.101.156, GigabitEthernet0/0/0/18 chassisId = 0. srcObjectDisplayName refers to the Location in EPNM UI. chassisId refers to Satellite Id in EPNMUI. If any of the above information is not populated, then corresponding value is not sent to NBI.	—
cenUserMessage2	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.22	User input message. This value can be configured. **Note** EPN manager does not support this field.	—
cenUserMessage3	SnmpAdminString	.1.3.6.1.4.9.9.311.1.1.2.1.23	User input message. This value can be configured. **Note** EPN manager does not support this field.	—
cenAlarmMode	Integer	.1.3.6.1.4.9.9.311.1.1.2.1.24	• unknown(1) —When the value for this attribute could not be determined. • alert(2) — Denotes an alarm generated by a set of events where all events are reported by polling of managed objects and/or listening to SNMP notifications. • event(3) — Denotes an event generated by polling of managed objects and/or listening to SNMP notifications.	2

SNMP Varbind	Data Type	Varbind OID	SNMP Varbing Description	Example
cenPartitionNumber	Integer	.1.3.6.1.4.1.9.9.311.1.1.2.1.24	In traps generated by the management application that support multiple partitions, the attribute will carry the integer value assigned to identify the logical group where the managed device resides. **Note** EPN manager does not support this field.	0
cenPartitionName	SnmpAdminString	.1.3.6.1.4.1.9.9.311.1.1.2.1.26	In traps generated by the management application that support multiple partitions, the attribute will carry the name assigned to identify the logical group where the managed device resides.	—
cenCustomerIdentification	SnmpAdminString	.1.3.6.1.4.1.9.9.311.1.1.2.1.27	User input message. The attribute takes in a free format text. This attribute can be used by advanced management applications to sort responses from the fault management server. **Note** EPN manager does not support this field.	—
cenCustomerRevision	SnmpAdminString	.1.3.6.1.4.1.9.9.311.1.1.2.1.28	User input message. The attribute takes in a free format text. This attribute can be used by advanced management applications to sort responses from the fault management server. **Note** EPN manager does not support this field.	—
cenAlertID	SnmpAdminString	.1.3.6.1.4.1.9.9.311.1.1.2.1.29	In event based notification, this attribute will contain the alert id to which the generated event has been rolled upto. In alert based notification, the cenAlarmInstanceId and cenAlertID will be identical.	1185098114

Note Information in the alarm that is null will not be forwarded to NBI.

Cisco EPM Notification MIB



APPENDIX D

Monitoring Policies Reference

The following topics describe the monitoring policies used by Cisco EPN Manager. For information on the supported MIBs and MIB objects, see Cisco EPN Manager.

Device Health Monitoring Policy

The Device Health Monitoring Policy monitors device CPU utilization, memory pool utilization, environmental temperature, and device availability for all devices in the network. By default, the policy polls devices for this information every 5 minutes, and an alarm is generated if CPU utilization, memory pool utilization, or environmental temperature thresholds are surpassed.

This monitoring policy is activated by default after installation.

Note This policy does not monitor the device CPU utilization and memory pool utilization for supported Cisco ONS or Cisco NCS 2000 devices, but it does monitor memory utilization and device availability.

For information on how to manage this policy, see Set Up Basic Device Health Monitoring, on page 224.

Note A Device Health Monitoring Policy should not have more than 100 devices under it. For example, if you want to add more than 100 cBR-8 devices in Cisco Evolved Programmable Network Manager, best approach is to create multiple policies and split the devices amongst them.

Interface Health Monitoring Policy

An Interface Health Monitoring Policy monitors over 30 attributes to check interface operational status and performance. It polls device interfaces every 5 minutes and generates an alarm when interface discard, error, utilization, or byte rate thresholds are exceeded.

To protect the performance of large deployments, this policy is not activated by default.

Note This policy does not monitor optical interfaces. Use an optical policy to monitor that information. See Optical 1 day, Optical 15 mins, and Optical 30 secs Monitoring Policies, on page 956.

See these topics for information on how to manage this policy:

- To check whether an Interface Health policy is actively monitoring interfaces, see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To set up interface monitoring, see Set Up Basic Interface Monitoring, on page 225.
- To adjust an interface monitoring policy, see Adjust What Is Being Monitored, on page 230.

Custom MIB Polling Monitoring Policy

The Custom MIB Polling monitoring policy is a customizable policy that you can use to monitor unsupported parameters—that is, parameters that are not polled by any of the existing monitoring policy types. While creating a custom MIB polling policy, you can choose from an extensive list of Cisco and other MIBs, or import new MIBs into the policy. For more information on managing Custom MIB Polling monitoring policies, see the following topics:

- To check if a custom MIB polling policy is being used to monitor information, see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new custom MIB polling policy, see Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 232.
- To adjust an existing custom MIB polling policy, see Adjust What Is Being Monitored, on page 230.

- To schedule and generate custom MIB reports, see Schedule Custom MIB reports, on page 233

IP SLA Y.1731 Monitoring Policy

An IP SLA Y.1731 monitoring policy uses the Y.1731 ITU-T recommendation to monitor over 70 fault and performance attributes in Metro Ethernet networks.

When you create an IP SLA Y.1731 monitoring policy, by default, it polls the parameters every 15 minutes (by default) and generates an alarm when delay, jitter, frame loss, ccm frame loss, and other thresholds are exceeded.

Cisco EPN Manager stores data at the same interval at which data is stored in the history bucket of the device. For example, if the history buckets on the device are updated every 5 mins and the monitoring policy is configured to poll the device every 15 minutes, Cisco EPN Manager stores 3 buckets of data every 15 minutes.

To collect all polled data without any bucket:

1. Ensure that time interval of the aggregated history buckets is longer than the polling interval of the monitoring policy.
2. Configure at least two history buckets on the device.

This enhancement is available in:

- Cisco IOS-XR devices that run 6.1.1 OS version and higher. Data collection for all probe types (loss and delay) must be triggered at the same time for all devices. All devices must be configured with the same history bucket duration.
- Cisco IOS-XE devices - NCS 42xx and NCS 520 devices that run 17.3.1 OS version and higher.

Note For devices where this enhancement is not applicable (devices running an older software version or with the collection conditions mentioned above not met), Cisco EPN Manager collects and aggregates data from relevant buckets according to the policy collection interval.

For each measurement, the forward, backward and two way data is collected. Bins statistics data is not polled by default. To enable the collection of this data, choose a polling frequency, for details see Change the Polling for a Monitoring Policy.

Note This policy collects Bins statistics data on ME 1200, NCS 42xx and ASR 9xx devices.

For ME 1200 devices, if the MEG ID is longer than 18 characters, Bin statistics data will not be collected and presented in the Y1731 dashboard tab.

For more information on how to configure and manage an IP SLA Y.1731 monitoring policy, see these topics:

- To check if IP SLA Y.1731 parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new IP SLA Y.1731 monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.

- To adjust an existing IP SLA Y.1731 monitoring policy, see Adjust What Is Being Monitored, on page 230.

Pseudowire Emulation Edge to Edge Monitoring Policy

A Pseudowire Emulation Edge to Edge (PWE3) monitoring policy polls approximately 20 attributes that emulate edge-to-edge services over a Packet Switched Network (PSN). When you create and enable a monitoring policy that uses this policy type, attributes are polled every 15 minutes by default. In addition, Cisco Evolved Programmable Network Manager generates a minor alarm when the thresholds for the following attributes are surpassed on pseudowire virtual circuits (PW VCs):

- HC packets and bytes—Total in and total out rates
- Operational status up, inbound and outbound operational status up

For more information on how to configure and manage a PWE3 monitoring policy, see these topics:

- To check if PWE3 parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new PWE3 monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.
- To adjust an existing PWE3 monitoring policy, see Adjust What Is Being Monitored, on page 230.

PTP/SyncE Monitoring Policy

The PTP/SyncE monitoring policy measures PTP and SyncE performance. When you create a PTP/SyncE Monitoring policy, it polls the parameters every 30 minutes by default. The polling frequency can also be set to 5 , 15 or 60 minutes.

For more information on how to configure and manage a PTP/SyncE monitoring policy, see these topics:

- To check what the PTP/SyncE monitoring policy is monitoring , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new PTP/SyncE monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.
- To adjust an existing PTP/SyncE monitoring policy, see Adjust What Is Being Monitored, on page 230.

Quality of Service Monitoring Policy

A Quality of Service monitoring policy polls over 60 service parameters to validate the quality of services running on network devices. When you create a Quality of Service monitoring policy, it polls the parameters every 15 minutes and generates an alarm when certain thresholds are exceeded. The following is a partial list of parameters that can cause an alarm:

- Dropped/discarded bytes and packets rates

- Pre-policy bytes and packets rates, utilization, percent of Committed Information Rate (CIR), Peak Information Rate (PIR)
- Post-policy bytes rates, utilization, percent of Committed Information Rate (CIR), Peak Information Rate (PIR)

To view all Quality of Service parameters that can cause TCAs, see Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 229.

For more information on how to configure and manage a Quality of Service monitoring policy, see these topics:

- To check if Quality of Service parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new Quality of Service monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.
- To adjust an existing Quality of Service monitoring policy, see Adjust What Is Being Monitored, on page 230.

IP SLA Monitoring Policy

An IP SLA monitoring policy monitors approximately 20 parameters to provide real-time performance information. When you create an IP SLA monitoring policy, it polls the parameters every 15 minutes. This monitoring policy does not generate any alarms; if you want to generate IP SLA-based alarms, use the IP SLA Y.1731 monitoring policy.

For more information on how to configure and manage an IP SLA monitoring policy, see these topics:

- To check if IP SLA parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new IP SLA monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.
- To adjust an existing IP SLA monitoring policy, see Adjust What Is Being Monitored, on page 230.

ME1200 EVC QoS Monitoring Policy

A ME1200 QoS monitoring policy polls 28 service parameters to validate the quality of selected services running on ME1200 devices. When you create a ME1200 Quality of Service monitoring policy, it polls the parameters every 15 minutes by default but does not generate an alarm when certain thresholds are exceeded. The polling frequency can be changed by selecting the preferred value from the drop down list.

The following is a partial list of parameters that are polled by ME1200 QoS monitoring policy:

- Transmitted and discarded bytes and packets rates.
- Average bit and frame rates for green (conforming), yellow (exceeding), red (violating), and discard traffic (both inbound and outbound)

Note To ensure that you are viewing accurate ME1200 QoS data, when you enable the ME1200 EVC Quality of Service monitoring policy, first disable the EVC performance monitoring session on the ME1200 devices.

To view all ME1200 QoS parameters that are polled, see Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 229.

For more information on how to configure and manage a ME1200 QoS monitoring policy, see these topics:

- To check if ME1200 QoS parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new ME1200 QoS monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.
- To adjust an existing ME1200 QoS monitoring policy, see Adjust What Is Being Monitored, on page 230.

MPLS Link Performance Monitoring Policy

The MPLS Link Performance monitoring policy measures link delay in MPLS. When you create a MPLS link performance Monitoring policy, it polls the parameters every 15 minutes by default. The polling interval can also be set to 1, 5 or 60 minutes.

Note This policy collects data on the following devices:

- For Link delay:
  - ASR 9000 devices, version 7.0.1 and above.
  - NCS 5500 devices , version 7.1.1 and above .
- For TWAMP Light responder metrics:
  - ASR 9000 devices, version 7.0.1 and above.
  - NCS 540 devices, version 7.2.1 and above.

This policy polls the following parameters:

- Average Delay
- Min Delay
- Max Delay
- RX packets
- TX packets

For more information on how to configure and manage a MPLS Link Performance monitoring policy, see these topics:

- To check what the MPLS Link Performance monitoring policy is monitoring , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new MPLS Link Performance monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.
- To adjust an existing MPLS Link Performance monitoring policy, see Adjust What Is Being Monitored, on page 230.

BNG Sessions and IP Pools Monitoring Policy

This monitoring policy polls over 5 parameters to monitor the BNG sessions as well as the IP addresses leased from the IP pools. When you create a BNG Sessions and IP Pools monitoring policy, it polls the parameters every 15 minutes and generates an alarm when certain thresholds are exceeded. The following is a partial list of parameters that can cause an alarm:

- Number of used or free IP addresses in the IP pools.
- Number of sessions for authenticated and up subscribers.

To view all BNG Sessions and IP Pools parameters that can cause TCAs, see Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 229.

For more information on how to configure and manage a BNG Sessions and IP Pools monitoring policy, see these topics:

- To check if BNG Sessions and IP Pools parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new BNG Sessions and IP Pools monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.
- To adjust an existing BNG Sessions and IP Pools monitoring policy, see Adjust What Is Being Monitored, on page 230.

TDM/SONET Ports Monitoring Policy

When you create a TDM/SONET Ports monitoring policy, it polls the parameters based on the polling frequency selected. You can define alarms that will be generated if any thresholds parameters are exceeded.

For more information on how to configure and manage a TDM/SONET Ports monitoring policy, see these topics:

- To check if TDM/SONET Ports parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new TDM/SONET Ports monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.

- To adjust an existing TDM/SONET Ports monitoring policy, see Adjust What Is Being Monitored, on page 230.

Optical SFP Monitoring Policy

An Optical SFP monitoring policy polls health and performance information for optical Small Form-Factor Pluggable (SFP) interfaces. This policy polls temperature, voltage, current, and optical TX/RX power. When you create an Optical SFP monitoring policy, it polls the parameters every 1 minute.

For more information on how to configure and manage an Optical SFP monitoring policy, see these topics:

- To check if Optical SFP parameters are being monitored , see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new Optical SFP monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.
- To adjust an existing Optical SFP monitoring policy, see Adjust What Is Being Monitored, on page 230.

Optical 1 day, Optical 15 mins, and Optical 30 secs Monitoring Policies

The Optical 1 day monitoring policy poll the following optical interfaces:

- Physical, OTN, Ethernet, and SONET/SDH interfaces on Cisco NCS 4000, ASR 9K, NCS 55xx, and NCS 1K devices.
- DWDM interfaces on Cisco NCS 2000 and Cisco ONS devices.

The Optical 15 mins monitoring policy poll the following optical interfaces:

- Physical, OTN, OTU FEnd, OTU NEnd, ODU FEnd, ODU NEnd, OTN GFP, OTN FEC, Ethernet, and SONET/SDH interfaces on Cisco NCS 4000, ASR 9K, NCS 55xx, NCS 57xx, CISCO 8xxx, and NCS 1K devices.
- DWDM interfaces on Cisco NCS 2000 and Cisco ONS devices.

The Optical 30 secs monitoring policy polls the Physical, OTN, and Ethernet parameters on the Cisco NCS 1001 and NCS 1004 devices.

See Performance Counters for Optical Monitoring Policies, on page 958 for a list of the parameters that these policies poll.

For more information on how to configure and manage the Optical 1 day, Optical 15 mins, and Optical 30 secs monitoring policy, see the following topics:

- To check if Optical 1 day, Optical 15 mins, and Optical 30 secs parameters are being monitored, see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new Optical 1 day, Optical 15 mins, and Optical 30 secs monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.

- To adjust an existing Optical 1 day, Optical 15 mins, and Optical 30 secs monitoring policy, see Adjust What Is Being Monitored, on page 230.

Note For IOS-XR devices, you can generate a collected OTN 15 mins report or choose a specific OTN 15 mins parameter to generate separate configuration reports. The different options are:

- OTU FEnd
- OTU NEnd
- ODU FEnd
- ODU NEnd
- OTN GFP
- OTN FEC

CEM Monitoring Policy

Use the CEM Monitoring Policy to poll the following CEM parameters:

- Jitter Buffer Overruns
- Generated Lbits
- Received Lbits
- Generated Rbits
- Received Rbits
- Generated Nbits
- Received Nbits
- Generated Pbits
- Received Pbits

The polling happens through the CLI and the delta of the current and last collection is taken as the current entry.

Note This polling data is not displayed in the dashboard.

Device Sensor Monitoring Policy

Use the Device Sensor monitoring policy to poll the sensor information through SNMP to the devices that are added to this policy. The sensor details such as voltage, power, and current temperature are polled to the device.

Note There are no calculations involved in the device sensor data.

Performance Counters for Optical Monitoring Policies

The following topics list the performance counters used by the optical monitoring policies. This information is provided here because it is not available from the web GUI.

- Reference—Performance Counters for Physical Interfaces, on page 958
- Reference—Performance Counters for OTN-FEC Interfaces, on page 961
- Reference—Performance Counters for OTN-ODU Interfaces, on page 961
- Reference—Performance Counters for OTN-OTU Interfaces, on page 962
- Reference—Performance Counters for Ethernet Interfaces, on page 963
- Reference—Performance Counters for SONET Interfaces, on page 964
- Reference—Performance Counters for SDH Interfaces, on page 965
- Reference—Performance counters for DS1/DS3, on page 967

Reference—Performance Counters for Physical Interfaces

The following table lists the performance counters used by the optical policy types to monitor physical interfaces.

Performance counters marked with an asterisk (*) are applicable for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices. Performance counters marked with a double asterisk (**) are applicable for Cisco Network Convergence System (NCS) 4000 series devices.

Physical Interface Performance Counter	Description
OPR-MIN	Minimum output power received by the optical circuit.
OPR-AVG	Average output power received by the optical circuit.
OPR-MAX	Maximum output power received by the optical circuit.
OPT-MIN	Minimum output power transmitted from the optical circuit.
OPT-AVG	Average output power transmitted from the optical circuit.

OPT-MAX	Maximum output power transmitted from the optical circuit.
OSC_PWR	Power received by the optical circuit.
LBC-MIN* LBCL-MIN	Minimum laser bias current for the optical circuit.
LBC-AVG* LBCL-AVG	Average laser bias current for the optical circuit.
LBC-MAX* LBCL-MAX	Maximum laser bias current for the optical circuit.
DGD-MIN**	Minimum differential group delay for the optical circuit.
DGD-AVG**	Average differential group delay for the optical circuit.
DGD-MAX**	Maximum differential group delay for the optical circuit.
SOPMD-MIN**	Minimum second order polarization mode dispersion for the optical circuit.
SOPMD-AVG**	Average second order polarization mode dispersion for the optical circuit.
SOPMD_MAX**	Maximum second order polarization mode dispersion for the optical circuit.
OSNR-MIN**	Minimum optical signal to noise ratio for the optical circuit.
OSNR-AVG**	Average optical signal to noise ratio for the optical circuit.
OSNR-MAX**	Maximum optical signal to noise ratio for the optical circuit.
eSNR-MIN**	Minimum electrical signal to noise ratio for the optical circuit.
eSNR-AVG**	Average electrical signal to noise ratio for the optical circuit.
eSNR-MAX**	Maximum electrical signal to noise ratio for the optical circuit.
PDL-MIN**	Minimum polarization-dependent loss for the optical circuit.
PDL-AVG**	Average polarization-dependent loss for the optical circuit.
PDL-MAX**	Maximum polarization-dependent loss for the optical circuit.
PCR-MIN**	Minimum polarization change rate for the optical circuit.
PCR-AVG**	Average polarization change rate for the optical circuit.
PCR-MAX**	Maximum polarization change rate for the optical circuit.
PMD-AVG*,**	Average polarization mode dispersion for the optical circuit.
PMD-MIN*,**	Minimum polarization mode dispersion for the optical circuit.

PN-MIN**	Minimum phase noise for the optical circuit.
PN-AVG**	Average phase noise for the optical circuit.
PN-MAX**	Maximum phase noise for the optical circuit.
PREFEC-BER*	Preforward error correction bit error rate for the optical circuit.
CD-MIN**	Minimum chromatic dispersion for the optical circuit.
CD-AVG**	Average chromatic dispersion for the optical circuit.
CD-MAX**	Maximum chromatic dispersion for the optical circuit.

Note PMD-MIN and PMD-AVG are not applicable for SVO devices.

The following table lists the performance counters used by the optical policy types to monitor physical interfaces and collect data in real time from NCS1004, NCS560, NCS5500, CISCO8XXX, NCS540 and ASR9K devices.

Physical Interface Performance Counter	**Description**
CD	Chromatic dispersion
DGD	Differential group delay
SOPMD	Second order polarization mode dispersion
PCR	Polarization change rate
PDL	Polarization-dependent loss
OSNR	Optical signal to noise ratio
TX-POWER	Optical power transmitted
RX-POWER	Optical power received
LBC	Laser Bias Current
RX-SIG	Received signal power
FREQ-OFF	Frequency Difference
Qfactor	Quality Factor
Qmargin	Quality Factor Margin
BAUDRATE	Rate of information transfer (bits per second)
Pre-FEC-Val	Pre Forward Error Correction Value

Pre-FEC-BER	Pre Forward Error Correction Value Bit Error Rate
Post-FEC-BER	Post Forward Error Correction Value Bit Error Rate

Reference—Performance Counters for OTN-FEC Interfaces

The following table lists the performance counters used by the optical policy types to monitor OTN-FEC interfaces.

Performance counters marked with an asterisk (*) are applicable for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices.

OTN-FEC Interface Performance Counter	**Description**
BIT-EC* BIEC	Number of bit errors corrected.
UNC-WORDS* UCW	Number of uncorrectable words.

Reference—Performance Counters for OTN-ODU Interfaces

The following table lists the performance counters used by the optical policy types to monitor OTN-ODU interfaces.

OTN-ODU Interface Performance Counter	**Description**
BBE-PM	Number of background block errors in path monitoring.
BBER-PM	Background block errors ratio in path monitoring.
ES-PM	Number of errored seconds in path monitoring.
ESR-PM	Errored seconds ratio in path monitoring.
SES-PM	Number of severely errored seconds in path monitoring.
SESR-PM	Severely errored seconds ratio in path monitoring.
UAS-PM	Number of unavailable seconds in path monitoring.
FC-PM	Number of failure counts (AIS/RFI detected) in path monitoring.
gfpStatsRxFrames	Number of generic framing procedure (GFP) frames received.
gfpStatsTxFrames	Number of GFP frames transmitted.
gfpStatsRxOctets	Number of GFP bytes received.
gfpStatsTxOctets	Number of GFP bytes transmitted.

gfpStatsRxCRCErrors	Number of packets received with a payload frame check sequence (FCS) error.
gfpStatsRxMBitErrors	Number of multiple bit errors. In the GFP core header at the GFP-transparent (GFP-T) receiver, these are uncorrectable.
gfpStatsRxSBitErrors	Number of single bit errors. In the GFP core header at the GFP-T receiver, these are correctable.
gfpStatsRxTypeInvalid	Number of packets received with invalid GFP type. This includes unexpected user payload identifier (UPI) type and errors in core header error check (CHEC).
gfpStatsRxCIDInvalid	Number of packets received with invalid CID.
gfpStatsRoundTripLatencyUSec	Round trip delay for the end-to-end Fibre Channel transport in milliseconds.
gfpStatsTxDistanceExtBuffers	Number of buffer credit transmitted for GFP-T transmitter (valid only if distance extension is enabled).
gfpStatsRxSblkCRCErrors	Number of super block cyclic redundancy check (CRC) errors.
gfpStatsCSFRaised	Number of GFP client signal fail (CSF) frames detected at the GFP-T receiver.
gfpStatsLFDRaised	Number of GFP loss of frame delineation (LFD) detected.
gfpRxCmfFrame	Number of client management frames (CMF) received.
gfpTxCmfFrame	Number of client management frames (CMF) transmitted.
gfpStatsCHecRxMBitErrors	Number of core header error control (cHEC) CRC multiple bit errors.
gfpStatsTHecRxMBitErrors	Number of type header error control (tHEC) CRC multiple bit errors.

Reference—Performance Counters for OTN-OTU Interfaces

The following table lists the performance counters used by the optical policy types to monitor OTN-OTU interfaces.

OTN-OTU Interface Performance Counter	**Description**
BBE-SM	Number of background block errors in section monitoring.
BBER-SM	Background block error ratio in section monitoring.
ES-SM	Number of errored seconds in section monitoring.
ESR-SM	Errored seconds ratio in section monitoring.
SES-SM	Number of severely errored seconds in section monitoring.

SESR-SM	Severely errored seconds ratio in section monitoring.
UAS-SM	Number of unavailable seconds in section monitoring.
FC-SM	Number of failure counts (AIS/RFI detected) in section monitoring.

Reference—Performance Counters for Ethernet Interfaces

The following table lists the performance counters used by the optical policy types to monitor Ethernet interfaces.

Ethernet Interface Performance Counter	Description
ifInOctets	The total number of octets received on the interface, including framing octets.
ifInErrors	The total number of received packets that were discarded because of errors.
ifOutOctets	The total number of transmitted octets, including framing packets.
ifInUcastPkts	The total number of unicast packets received since the last counter reset.
ifOutUcastPkts	The total number of packets requested by the higher-level protocols to be transmitted, and which were not addressed to a multicast or broadcast address at this sub-layer, including those that were discarded or not sent.
ifInMulticastPkts	The total number of multicast packets received since the last counter reset.
ifOutMulticastPkts	The total number of multicast frames transmitted error free.
ifInBroadcastPkts	The total number of broadcast packets received since the last counter reset.
ifOutBroadcastPkts	The total number of packets requested by higher-level protocols and addressed to a broadcast address at this sublayer, including those that were not transmitted.
txTotalPkts	The total number of packets transmitted.
rxTotalPkts	The total number of packets received.
etherStatsOctets	The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octets).
etherStatsOversizePkts	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets) and were otherwise well formed. Note that for tagged interfaces, this number becomes 1522 bytes.
dot3StatsFCSErrors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check.
dot3StatsFrameTooLongs	A count of frames received on a particular interface that exceed the maximum permitted frame size.

etherStatsJabbers	The total number of packets received that were longer than 1518 octets (excluding framing bits but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
etherStatsPkts64Octets	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
etherStatsPkts65to127 Octets	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts128to255 Octets	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts256to511 Octets	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts512to1023Octets	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsPkts1024to1518Octets	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
etherStatsMulticastPkts	The total number of good packets received that were directed to a multicast address.
etherStatsBroadcastPkts	The total number of good packets received that were directed to the broadcast address.
etherStatsUndersizePkts	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

Reference—Performance Counters for SONET Interfaces

The following table lists the performance counters used by the optical policy types to monitor SONET interfaces.

Performance counters marked with an asterisk (*) are applicable for all Cisco Optical Networking Services (ONS) and Cisco Network Convergence System (NCS) 2000 series devices.

SONET Interface Performance Counter	Description	Available over
Errored Seconds (ES)*	Number of errored seconds for near end and far end devices.	Line* Path VT-Path

SONET Interface Performance Counter	Description	Available over
		Section* (applicable only for near end devices)
Severely Errored Seconds (SES)*	Number of severely errored seconds for near end and far end devices.	Line* Path VT-Path Section* (applicable only for near end devices)
Severely Errored Framing Seconds (SEFS)*	Number of severely errored framing seconds for near end devices.	Section* (applicable only for near end devices)
Coding Violations (CV)*	Number of coding violations for near end and far end devices. .	Line* Path VT-Path Section* (applicable only for near end devices)
Unavailable Seconds (UAS)*	Number of unavailable seconds for near end and far end devices.	Line* Path VT-Path

Reference—Performance Counters for SDH Interfaces

The following table lists the performance counters used by the optical policy types to monitor SDH interfaces.

SDH Interface Performance Counter	Description
MS-ES	Number of errored seconds per multiplex section for near end and far end devices.
MS-ESR	Error seconds ratio per multiplex section for near end and far end devices.
MS-SES	Number of severely errored seconds per multiplex section for near end and far end devices.
MS-SESR	Severely errored seconds ratio per multiplex section for near end and far end devices.
MS-BBE	Number of background block errors per multiplex section for near end and far end devices.
MS-BBER	Background block error ratio per multiplex section for near end and far end devices.
MS-UAS	Number of unavailable seconds per multiplex section for near end and far end devices.

Monitoring Policies Reference

MS-EB	Number of errored block per multiplex section for near end and far end devices.
MS-FC	Number of failure counts per multiplex section for near end and far end devices.
MS-PSC	Protection switching count per multiplex section. PSC is the number of times the service switches from a working card to a protection card and back.
MS-PSC-R	Protection switching count ring per multiplex section. This count is incremented only if ring switching is used.
MS-PSC-S	Protection switching count span per multiplex section. This count is incremented only if span switching is used.
MS-PSC-W	Protection switching count working per multiplex section. It is the count of the number of times traffic switches away from the working capacity in the failed line and back to the working capacity after the failure is cleared. PSC-W increments on the failed working line.
MS-PSD	Protection switching duration applies to the length of time, in seconds, that service is carried on another line.
MS-PSD-R	Protection switching duration ring is a count of the seconds that the protection line was used to carry service. This count is incremented only if ring switching is used.
MS-PSD-S	Protection switching duration span is a count of the seconds that the protection line was used to carry service. This count is incremented only if span switching is used.
MS-PSD-W	Protection switching duration working per multiplex section.
RS-ES	Number of errored seconds per regenerator section.
RS-ESR	Errored seconds ratio per regenerator section.
RS-SES	Number of severely errored seconds per regenerator section.
RS-SESR	Severely errored seconds ratio per regenerator section.
RS-BBE	Number of background block errors per regenerator section.
RS-BBER	Background block errors ratio per regenerator section.
RS-UAS	Number of unavailable seconds per regenerator section.
RS-EB	Number of errored block per regenerator section.
RS-OFS	Number of out-of-frame seconds per regenerator section.

Reference—Performance counters for DS1/DS3

Performance counters for DS1

DS1 Performance Counter	Description
Unavailable Seconds (UAS)	Number of unavailable seconds for near end and far end devices.
Code Violations (CV)	Number of code violations for near end and far end devices.
Controlled Slip Seconds (CSS)	Number of controlled slip seconds for near end and far end devices.
Errored Seconds (ES)	Number of errored seconds for near end and far end devices.
Severely Errored Seconds (SES)	Number of severely errored seconds for near end and far end devices.
Severely Errored Framing Seconds (SEFS)	Number of severely errored framing seconds for near end and far end devices.
Bursty Error Seconds (BES)	Number of bursty error seconds for near end and far end devices.
Degraded Minutes (DM)	Number of degraded minutes for near end and far end devices.

Performance Counters for DS3

DS3 Performance Counter	Description
Errored Seconds (ES)	Number of errored seconds for near end and far end devices.
Severely Errored Seconds (SES)	Number of severely errored seconds for near end devices.
Code Violations (CV)	Number of code violations for near end and far end devices.
P-bit Code Violations (CVP)	Number of P-bit code violations for near end devices.
P-bit Errored Seconds (ESP)	Number of P-bit errored seconds for near end devices.
Severely Errored Seconds P-bit (SESP)	Number of P-bit severely errored seconds for near end and far end devices.
Severely Errored Framing Seconds (SEFS)	Number of severely errored framing seconds for near end devices.
Unavailable Seconds (UAS)	Number of unavailable seconds for near end and far end devices.
C-bit Coding Violations (CVC)	Number of C-bit coding violations for near end and far end devices.

DS3 Performance Counter	Description
C-bit Errored Seconds (ESC)	Number of C-bit errored seconds for near end and far end devices.
Severely Errored Seconds CP-bit (SESCP)	Number of CP-bit severely errored seconds for near end and far end devices.

GNSS Monitoring Policy

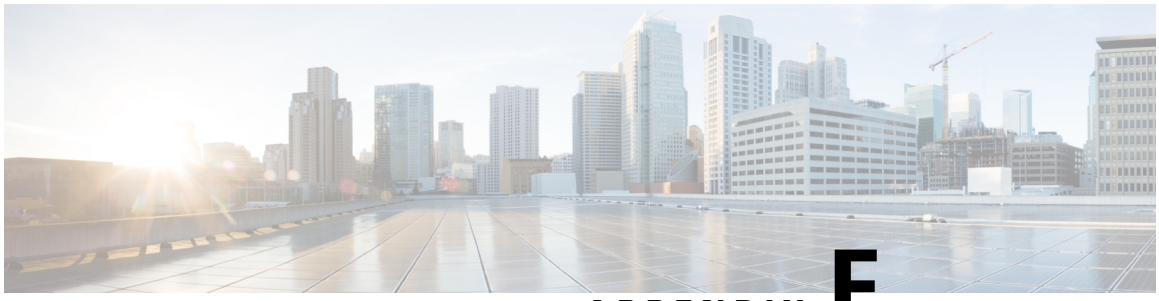
When you create a Global Navigation Satellite System (GNSS) monitoring policy, Cisco EPN Manager collects data from a network device by polling the following parameters:

- GNSS Module Presence Status
- GNSS Module Slot State
- GNSS Satellite Visibility Status
- GNSS Module Satellite Count
- GNSS Module SvId SNR
- GNSS Antenna Short Alarm Status
- GNSS Antenna Open Alarm Status

The policy polls every 30 minutes by default. You can change the default interval by changing the polling frequency. Note that GNSS monitoring policy does not have a threshold crossing alarm.

For more information on how to configure and manage GNSS monitoring policy, see these topics:

- To check what the GNSS monitoring policy is monitoring, see Check What Cisco Evolved Programmable Network Manager Is Monitoring, on page 228.
- To create a new GNSS monitoring policy, see Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 232.
- To adjust an existing GNSS monitoring policy, see Adjust What Is Being Monitored, on page 230.



APPENDIX E

Cisco Evolved Programmable Network Manager RESTful API

Cisco Evolved Programmable Network Manager SDK

The Cisco Evolved Programmable Network Manager SDK is a collection of technologies that enables you to extend the capabilities of Cisco Evolved Programmable Network Manager, access data, and invoke the automation operations from any application. The Cisco Evolved Programmable Network Manager SDK includes the RESTful APIs and Open Automation. It is possible to use the RESTful API with scripting languages such as "bash with wget and cURL utilities", "Python", "Ruby", Java and so on.

With Cisco Evolved Programmable Network Manager SDK technologies, you can:

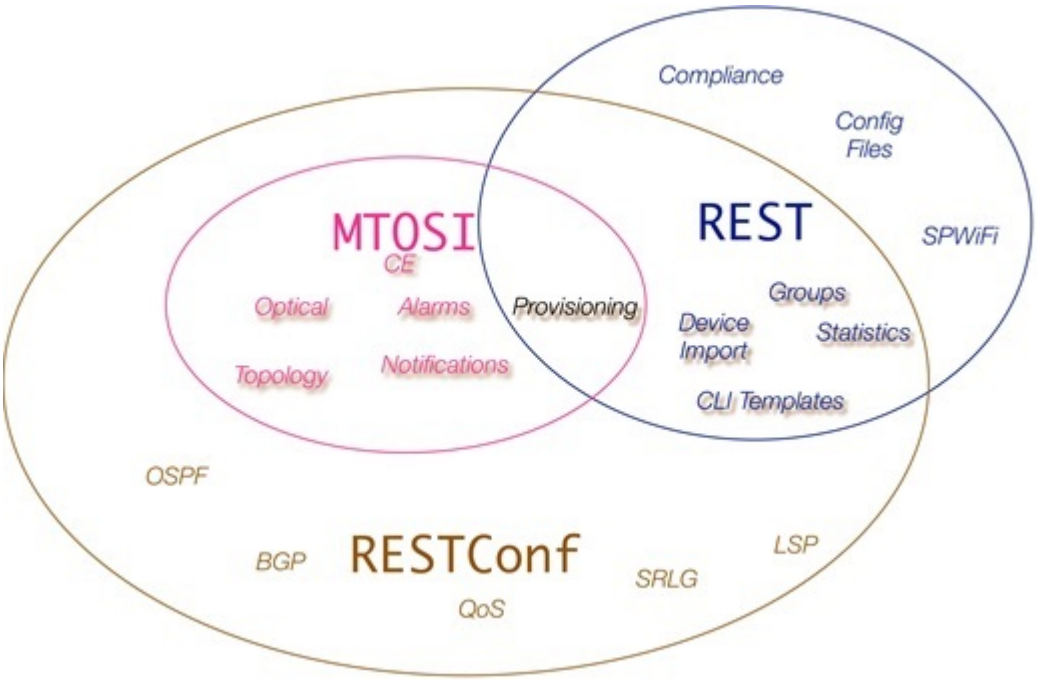
- Access Cisco Evolved Programmable Network Manager programmatically—Use the Cisco Evolved Programmable Network Manager RESTful API to invoke workflows and obtain reports.
- Customize Cisco Evolved Programmable Network Manager —Create custom workflow tasks, Customize Cisco Evolved Programmable Network Manager by deploying your own jar files and script libraries in script modules. Use custom tasks from script bundles.

Cisco Evolved Programmable Network Manager APIs

Cisco Evolved Programmable Network Manager provides easy to use and comprehensive APIs that allow integration with any standards-based OSS system north bound. These APIs extend its core functionalities using three of the most commonly used standards - MTOSI and RESTConf, and RESTful APIs.

To provide rapid development design for automation, it is important for developers to develop APIs consistently thus paving way for a smoothest and easy to use design guidelines. Consistency allows teams to leverage common code, patterns, documentation and design decisions. In Cisco Evolved Programmable Network Manager, RESTful APIs are easily made available within the application with simple and extensive examples. The following diagram is an example that illustrates the general behavior found in Cisco Evolved Programmable Network Manager across *all* its APIs.

Figure 17: EPNM RESTful API General Behavior



This chapter is intended for the following technical professionals interested in using the Cisco Evolved Programmable Network Manager Development Kit (SDK) and related technologies. Such users might be:

- System administrators and REST API developers who use Cisco Evolved Programmable Network Manager and want to extend their ability to automation resources using it.
- Anyone else who wants to compare Cisco Evolved Programmable Network Manager SDK or API technologies and determine which would be most appropriate for their application

Cisco Evolved Programmable Network Manager provides three northbound API interface types, MTOSI, REST and RESTConf. The functionality provided by these three APIs are fairly similar but not all APIs provide the same functions.

The MTOSI API is the most different of the APIs in terms of behavior. It provides a SOAP interface over HTTPS that provides basic provisioning of optical and carrier ethernet functionality. Use the MTOSI interface if you need to provision optical services such as DWDM or OTN, and cannot use the RESTConf API.

The REST API provides system information and most statistics and assurance information besides other functions that handle configuration files, group management and device import capabilities.

The RESTConf API, like the above REST API, adheres to a RESTful interface. It provides all provisioning for carrier ethernet, L2/L3 VPNs, circuit emulation, OTN and DWDM technologies as well as core routing and switching.

For more information see the individual Cisco EPNM integration guides available on cisco.com.

When to Use Cisco Evolved Programmable Network Manager RESTful API

Cisco Evolved Programmable Network Manager RESTful API is a language-independent interface that can be used by any program or script capable of making HTTP requests. Use the REST API when you want to invoke operations on Cisco Evolved Programmable Network Manager from a separate program or process.

Applications can use the RESTful API to do the following:

- Retrieve Cisco Evolved Programmable Network Manager reports on physical and virtual devices, networks, appliances, groups and users, policies, and other monitored entities within your Cisco Evolved Programmable Network Manager domains.
- Invoke additional operations specific to Cisco Evolved Programmable Network Manager.

How to Use Cisco Evolved Programmable Network Manager RESTful API

Because a RESTful API client interacts with Cisco Evolved Programmable Network Manager using standard HTTP requests and responses, the RESTful API responses are compatible with any web browser. Many programming languages have libraries that are devoted to creating and sending HTTP requests and handling HTTP responses.

Most of the REST API calls send and return data in the request or the response, respectively. These data payloads may be formatted in one of two ways depending on the RESTful API call. Some of the RESTful API calls use a JavaScript Object Notation (JSON) payload, while others use an XML payload. You probably have to use both for any reasonably complex application.

A JSON-based RESTful API call is a plain HTTP request and response with a JSON payload. JSON is a lightweight text-based open standard that is designed for human-readable data interchange. JSON represents simple data structures and associative arrays. Your application directly invokes the JSON-based API without using any specialized RESTful API libraries, and parses JSON data using any means native to your application.

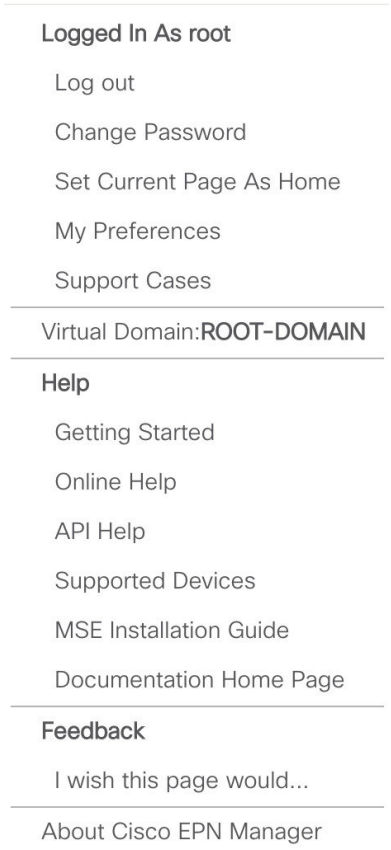
All requests to the Cisco Evolved Programmable Network Manager API require user authentication. For more information about Authentication, see Authentication and Authorization.

Authorization in the RESTful API is enforced by requiring that only registered users of Cisco Evolved Programmable Network Manager are able to make API requests. For Cisco Evolved Programmable Network Manager, access to the API is controlled by three user groups such as NBI Read and NBI Write. Each of these groups controls access to a different set of APIs. You can assign a user to multiple groups if you wish. You can check the documentation page of an API resource to determine which user group is required to access it. When a user is created and registered on Cisco Evolved Programmable Network Manager, the user is assigned a unique RESTful API access key.

To obtain the RESTConf topological link retrieval resources, you can use RESTful topological link resources to get these values and perform the required correlation.

To access Cisco Evolved Programmable Network Manager RESTful API documentation:

- Launch Cisco Evolved Programmable Network Manager, and then in the top-right corner, click ⚙, the window settings menu opens.



- Choose **Help** > **API Help** > **REST API** to learn about system requirements, how to set up a development environment, how to install libraries, usage of RESTful APIs, the list of every Cisco Evolved Programmable Network Manager REST API function, REST API Resources, different use case examples, queries, and so on.

RESTConf API-An Overview

In Cisco EPN Manager, the implementation conforms to the RESTConf/Yang specification information model and operational APIs protocols. Where required, the information model and operations APIs are extended in a standard way to support Cisco's vendor extensions to the RESTConf/Yang interface. These extensions are added as a set of xml and yang schema definitions for the information model extensions.

RESTCONF—Uses structured data (XML or JSON) and YANG to provide a REST-like APIs, enabling you to programmatically access different network devices. RESTCONF APIs use HTTPs methods.

YANG—A data modelling language that is used to model configuration and operational features . YANG determines the scope and the kind of functions that can be performed by NETCONF and RESTCONF APIs.

Following are the essential structure of RESTConf API:

- HTTP Headers: HTTP headers are used to describe the content sent or requested within an HTTP request. HTTP headers include:
  - Content-Type: At server side, an incoming request may have an entity attached to it. To determine its type, server uses the HTTP request header Content-Type.
  - Accept: Similarly, to determine what type of representation is desired at client side, HTTP header ACCEPT is used. Generally, if no Accept header is present in the request, the server can send pre-configured default representation type.
- **HTTP Methods**: The following methods are used to call an API:
  - Get-The GET method is sent by the client to retrieve data and metadata for a resource.
  - Post-It is used to create a new entity, but it can also be used to update an entity. The POST method is sent by the client to create a data resource or invoke an operation resource.
  - Put-A PUT request is idempotent. The PUT method is sent by the client to create or replace the target data resource.
  - Delete-Request that a resource be removed. The DELETE method is used to delete the target resource.
- **Messages**: The RESTCONF protocol uses HTTP messages. A single HTTP message corresponds to a single protocol method.
- Media Types: XML and JSON.
- **Query Parameters:**
  - Content
  - Depth
  - Fields
  - Filter
  - Insert
  - Point
  - Start-time
  - Stop-time
  - With-defaults

Standard usage - Get Method

The “GET All RESTConf API calls” returns the existing endpoint schema sections.

GET /restconf/data/ietf-yang-library:modules-state

Retrieves all RESTConf API endpoints

The schema URLs provide the details for many of the enumeration variables as well as the structural components of the module.

Example for schema retrieval:

GET /restconf/schema/v1/cisco-resource-optical

Returns the YANG schema for the module as plain text.

Several URL parameters are often available in RESTConf API calls. These are not implemented in all calls.

- .maxCount
- .startIndex
- .depth

```
GET /restconf/data/v1/module:resource
The general format for a RESTConf GET call.
```

Table 67: Query Parameters

Query Parameter	Description
.depth (integer)	The number of detail levels to retrieve.
.maxCount (integer)	The limit of the number of rows retrieved.
.startIndex (integer)	The initial row to retrieve.

```
GET /restconf/data/v1/module:resource HTTP/1.1
```

RESTful API Utility

- Fully Distinguishable Name: Inventory objects in this interface has attributes representing FDN (Fully Distinguished Name). These attributes are used as identifiers of the object or as a reference to the object in query parameters or in the returns data wherever a reference to the object is needed. This FDN is a formatted string that consists of a set of type/value pairs with the following syntax, Sequence of <type>=<value> pairs separated by "!" where:
  - <type> is a constant value defined in the data model to represent the inventory object in the hierarchy, e.g. MD,ND,EQ,PTP,FTP, CTP, TL,VC,CFS, etc.
  - <value> is any text or sequence of <attrName>=<attrValue> pair separated by ";" that represents the attribute/value pairs of the inventory object constitutes a unique value within the local scope of the object represented by the type.

For more information, refer to the Cisco EPNM RESTConf guide.

RESTConf API Functional Areas

- Alarms—The alarms module provides mechanisms to retrieve and acknowledge alarms and events. The preferred method of managing alarms is to listen via the Notification API where a service can collect events of differing types or criticality and then handle them via this API.
- Performance Test—The Service Performance Test can be conducted standalone as well as part of service provisioning. Restconf NBI supports standalone performance test execution.
- Quality of Service (QoS)— QoS is a set of capabilities that allow the delivery of differentiated services for network traffic. Using Cisco EPN Manager you can configure QoS on Carrier Ethernet interfaces.

- OAM—The OAM tests in the EPNM RESTConf API fall into two general categories. The service and the network resource OAM configurations. For Y.1731, Y.1564 and BERT tests, the service-oam-config endpoint is used. For OTDR, the network-resource-oam-config endpoint is used. EPNM RESTConf OAM calls provide a POST command to initiate the test. That request yields a test ID and a test request ID. One usually then uses the test ID in a subsequent call to retrieve the results. There are URLs for most specific test types.
- Service Profiles—Service Profiles contain pre-defined provisioning request (order data) that can be used in provisioning each circuit/VC type. In NBI Provisioning request, a service profile reference can be used to get provisioning request data to be used in the provisioning. If the provisioning data is provided in the request along with the service profile reference, but the user provided data and the data stored in the service profile gets merged with user provided data overriding the profile data before the request is sent to execute provisioning. Service profile can be created using EPNM Service Profile wizard GUI.
- Customer Facing Services (CFS)—The CFS represents the customer facing data for a circuit/VC. The CFS is derived from discovered RFS and represents the endpoints of the circuit/VC in the network. During CFS discovery, the system creates CFS objects for the discovered RFS objects.
- Resource Facing Services (RFS)—The RFS represents the relations between resources on different devices. During RFS discovery, the system creates device-level objects and network-level objects. Device-level RFS objects represent the circuit/VC configuration parts of the device-level configuration. Network-level RFS objects aggregate device or other network-level objects to represent network-level entities.

Authentication and Authorization

All requests to the Cisco Evolved Programmable Network Manager API require user authentication. If no authentication details are provided in the request, the request is redirected to the login page. Authentication details may be passed through the HTTP header of the request. For more information see Authentication, Authorization, and Security topic (Home > Authentication, Authorization, and Security) in the Cisco Evolved Programmable Network Manager API documentation.

For Cisco EPN Manager, access to the API is controlled by the user groups such as NBI Read and NBI Write. Each of these groups controls access to a different set of APIs. You can assign a user to multiple groups if you wish. You can check the documentation page of an API resource to determine which user group is required to access it.

Note We recommended to use JSESSIONID during the production environment.

Getting Started with Cisco EPN Manager REST API

The Cisco Evolved Programmable Network Manager REST API allows an application to interact with Cisco Evolved Programmable Network Manager, programmatically. These requests provide access to resources in Cisco Evolved Programmable Network Manager. With an API call, you can execute Cisco Evolved Programmable Network Manager workflows and Monitor Alarms and Events, Collect device inventory, monitor network clients and usage, configure devices, Device Inventory and so on. For more information see,

the Getting Started topic (**Home** > **Getting Started**) in the Cisco Evolved Programmable Network Manager API documentation.

REST API Basics and Functional Areas

Cisco Evolved Programmable Network Manager's REST implementation uses multiple calls and filters. For example, when retrieving statistics, the first call provides URLs for the subsequent calls. Those then can be used for retrieving finer detail. In general, the URL parameters become more complicated with each call as more detail is added.

REST API Basics

- HTTPS Headers: The following HTTP Headers are used to control the way in which data is returned to a client.
  - Accept
  - Accept-Language
  - Content-Type
  - Accept-Encoding
  - Content-Encoding
- **Query Parameters:**

The API supports query parameters for almost all requests. The following table describes the General REST Query Parameters:

Table 68: General REST Query Parameters

Query Parameter	Applicability	Meaning
.json	/api/*	When present indicates that the response should be returned in json format.
.xml	/api/*	When present indicates that the response should be returned in xml format. This is the default in the absence of the .json parameter.
_docs	/api/*	Displays the documentation page.
.full	/api/v1/data/T	When 'true' indicates that whole objects be returned rather than just IDs of the entities.
.group	api/v1/data/T	Filters the response based on content of the group specified by the string value, and the result of any applied operator.

Query Parameter	Applicability	Meaning
.transform	GET/POST	Supplies the logical-name of a transform to be applied immediately before rendering to XML or JSON.
.maxresults	GET Paged	The greatest number of results in terms of the heads of instance trees returned.
.firstResult	GET Paged	The first result in terms of the heads of instance trees.
.strict	/api/v1/data/T	When ‘true’, the property names used in queries are validated, and an error thrown if appropriate. (The default - ie when strict=false - is to ignore invalid property names with a simple log message).
.case_sensitve	/api/v1/data/T	When ‘true’, the string values used in filter queries are case sensitive. (The default - ie when .case_sensitive=false - is to treat comparisons as case insensitive).
.nocount	/api/v1/data/T	When ‘true’, the “count”, “first”, and “last” attributes are not included the response. Getting the values of these attributes requires additional time, therefore setting this to ‘true’ will improve performance. Defaults to ‘false’.
_ctx.domain	GET	Sets the active domain to be that named in the query parameter value - this is, by default, “sticky” in the sense that once set, the active-domain remains set. The “stickiness” is not RESTful, and so it can be switched off in configuration.

REST API Functional Areas

- Statistics: The Statistics services provide summary, pre-defined statistical information about the system. Some of the resources of statistics are listed below.
  - GET All Border Routers
  - GET All IMEs
  - GET All RCs

- GET All TCAs
- GET All WANInterfaces

- Report Service: The Report service provides operations to discover and run reports. Reports need to be defined in the system prior to access through the API. The following APIs are supported:
  - GET Get Available Report Templates
  - (Deprecated) GET Get a Report
  - GET Get a ZIP Report
  - GET Run a ZIP Report

- CLI Template Configuration: The CLI Template Configuration service allows a CLI configuration template to be applied to one or more target devices. It also provides a way to upload, delete, and get the CLI templates in the system. The following APIs are supported:
  - GET CLI Configuration Templates
  - DELETE Delete Configuration Template
  - DELETE Delete Configuration Template Folder
  - GET Download Configuration Template
  - GET List Configuration Template Folders
  - GET List Configuration Templates
  - GET List Device Types
  - POST Create Configuration Template Folder
  - POST Upload Configuration Template
  - PUT Deploy Configuration Template
  - PUT Deploy Configuration Template Through Job
  - PUT Modify Configuration Template Content

Statistics

From EPNM you can acquire statistics data in a simple step by step process. This is a fairly consistent general pattern of usage across several REST statistics endpoints. In general, a high-level first call is made that returns a list of available metrics. From that call, a second list of finer statistics for a given metric is returned from which the actual data series is returned.

Following is an example for Statistics - endpoint call succession: ESR PM data for a given circuit:

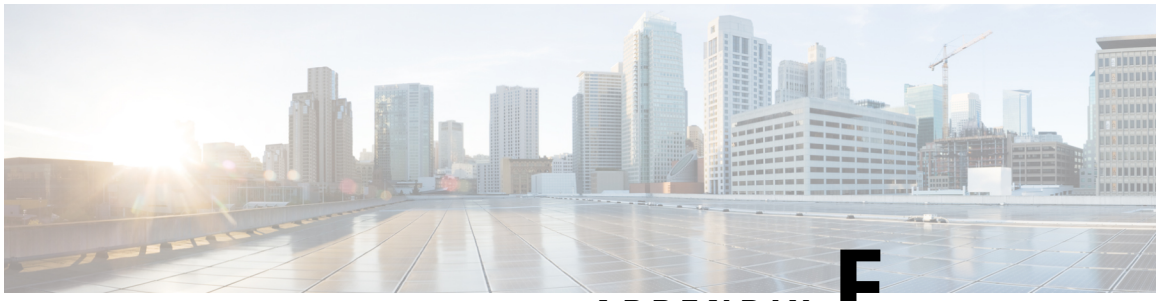
```
GET /webacs/api/v1/op/statisticsService/circuits?circuitName=VSO5_TO_HUB2
 GET
/webacs/api/v1/op/statisticsService/circuits/metrics?circuitType=ODUUNI&circuitId=161374613
```

Cisco Evolved Programmable Network Manager RESTful API

```
 GET
/webacs/api/v1/op/statisticsService/circuits/metrics/ESR_PM?maxResults=24&timeInterval=6&endpoint-
Name=ODU20/4/0/0/1&location=FEND&circuitType=ODUUNI&deviceId=124606492_10.201.1.174&circuitId=161374613
```

Note The URLs for the last two calls were provided in the body of the previous call.

Cisco Evolved Programmable Network Manager RESTful API



APPENDIX F

Supported and Unsupported Events for Event Flow Controllers

Supported Events

Following is the list of events that are monitored for burst and continuous events flow controllers.

Table 69: Supported Events

Technology	Events
MPLS	MPLS_TE-5-LSP_Down MPLS_TE-5-LSP_Active_StandBy MPLS_TE-5-LSP_CLEAR ROUTING-MPLS_TE-5-LSP_UPDOWN ROUTING-MPLS_TE-5-S2L_SIGNALLING_STATE
Pseudowire	cpwVcUp cpwVcDown L2-L2VPN_PW-3-UPDOWN L2-L2VPN_PW-3-UPDOWN_Clear XCONNECT-5-PW_STATUS XCONNECT-5-PW_STATUS_Clear EVPN-5-VC_STATUS EVPN-5-VC_STATUS_Clear
LDP	mplsLdpSessionDown mplsLdpSessionUp
OSPF	OSPF-5-ADJCHG OSPF-5-ADJCHG_DOWN OSPF-5-ADJCHG_UP OSPFv3-5-ADJCHG OSPFv3-5-ADJCHG_DOWN OSPFv3-5-ADJCHG_UP ROUTING-OSPF-5-ADJCHG ROUTING-OSPFv3-5-ADJCHG ROUTING-OSPFv3-5-ADJCHG_DOWN ROUTING-OSPFv3-5-ADJCHG_UP

Technology	Events
BGP	cbgpBackwardTransition cbgpFsmStateChange cbgpPrefixThresholdExceeded cbgpPrefixThresholdClear bgpBackwardTransition bgpEstablished cbgpPeer2BackwardTransition cbgpPeer2FsmStateChange cbgpPeer2FsmStateChangeUp cbgpPeer2FsmStateChangeDown cbgpPeer2PrefixThresholdClear cbgpPeer2PrefixThresholdExceeded BGP-5-ADJCHANGE BGP-5-ADJCHANGE_DOWN BGP-5-ADJCHANGE_UP BGP-3-NOTIFICATION ROUTING-BGP-5-ADJCHANGE ROUTING-BGP-5-UPDATE_FILTERED
ISIS	CLNS-5-ADJCHANGE CLNS-5-ADJCHANGE_UP CLNS-5-ADJCHANGE_DOWN ROUTING-ISIS-5-ADJCHANGE ROUTING-ISIS-5-ADJCHANGE_UP ROUTING-ISIS-5-ADJCHANGE_DOWN ROUTING-ISIS-4-ADJCHANGE ROUTING-ISIS-4-ADJCHANGE_UP ROUTING-ISIS-4-ADJCHANGE_DOWN isisAdjacencyChange isisAdjacencyChangeDown isisAdjacencyChangeUp isisAdjacencyChangeInit isisRejectedAdjacency

Unsupported Events

Following is the list of events that are not monitored for burst and continuous events flow controllers.

Table 70: Unsupported Events

Technology	Events
G8032	G8032-STATE_IDLE G8032-STATE_PENDING G8032-STATE_PROTECTION G8032-STATE_FORCED_SWITCH G8032-STATE_MANUAL_SWITCH L2-G8032-3-APS_CHANNEL_INACTIVE L2-G8032-6-APS_CHANNEL_ACTIVE

Technology	Events
CEM	SONET-4-ALARM_SLOS SONET-4-ALARM_SLOS_Clear SONET-4-ALARM_SLOF SONET-4-ALARM_SLOF_Clear SONET-4-ALARM_LAIS SONET-4-ALARM_LAIS_Clear SONET-4-ALARM_LRDI SONET-4-ALARM_LRDI_Clear SONET-4-ALARM_PAIS SONET-4-ALARM_PAIS_Clear SONET-4-ALARM_PLOP SONET-4-ALARM_PLOP_Clear SONET-4-ALARM_PUNEQ SONET-4-ALARM_PUNEQ_Clear SONET-4-ALARM_PPLM SONET-4-ALARM_PPLM_Clear SONET-4-ALARM_PRDI SONET-4-ALARM_PRDI_Clear SONET-4-ALARM_LOM SONET-4-ALARM_LOM_Clear SONET-4-ALARM_B1-TCA SONET-4-ALARM_B1-TCA_Clear SONET-4-ALARM_B2-TCA SONET-4-ALARM_B2-TCA_Clear SONET-4-ALARM_B3-TCA SONET-4-ALARM_B3-TCA_Clear SONET-4-ALARM_APS SONET-4-ALARM_APS_Clear SONET-4-UPSR_Working SONET-4-UPSR_Working_Clear SONET-4-UPSR_Protect SONET-4-UPSR_Protect_Clear CONTROLLER-5-UPDOWN_Clear CONTROLLER-5-UPDOWN dsx1LoopbackState dsx1LoopbackState_CLEAR dsx1RcvAIS dsx1RcvAIS_CLEAR dsx3RcvAIS dsx3RcvAIS_CLEAR dsx3LOS dsx3LOS_CLEAR dsx3LoopbackState dsx3LoopbackState_CLEAR dsx1LossOfSignal dsx1LossOfSignal_CLEAR SONET-4-ALARM_VT_TRACE_MISMATCH SONET-4-ALARM_VT_TRACE_MISMATCH_Clear SONET-4-ALARM_VT_PATH_LOP SONET-4-ALARM_VT_PATH_LOP_Clear SONET-4-ALARM_VT_UNEQUIPPED SONET-4-ALARM_VT_UNEQUIPPED_Clear SONET-4-ALARM_VT_PATH_RDI SONET-4-ALARM_VT_PATH_RDI_Clear CONTROLLER-5-UPDOWN_VT_PATHAIS CONTROLLER-5-UPDOWN_VT_PATHAIS_Clear CONTROLLER-5-UPDOWN_VT_PATHLOP CONTROLLER-5-UPDOWN_VT_PATHLOP_Clear CONTROLLER-5-UPDOWN_VT_UNEQUIPPED CONTROLLER-5-UPDOWN_VT_UNEQUIPPED_Clear

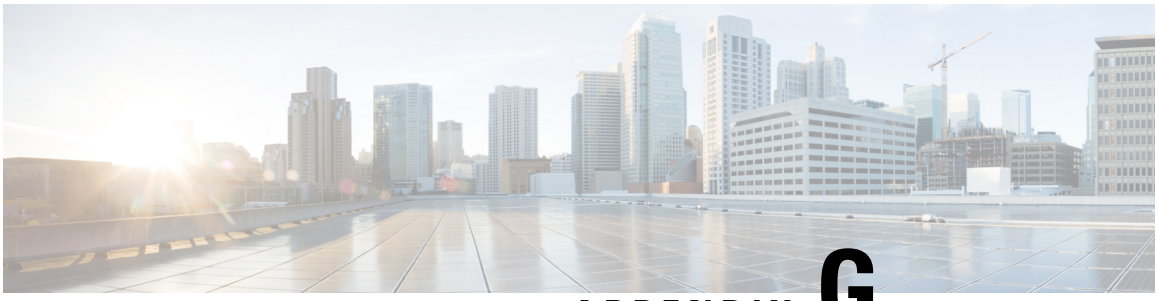
Supported and Unsupported Events for Event Flow Controllers

Technology	Events
	CONTROLLER-4-ACR_DCR_CLOCK_DS1 CONTROLLER-4-ACR_DCR_CLOCK_DS3 CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3 CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3 CONTROLLER-4-ACR_DCR_CLOCK_DS1_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_DS1_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_DS1_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_DS3_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_DS3_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_DS3_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_DS3_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_DS3_CHANNEL_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_OCN_VT_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_OCN_CT3_HOLDOVER CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_FREERUN CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_ACQUIRING CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_ACQUIRED CONTROLLER-4-ACR_DCR_CLOCK_OCN_T3_HOLDOVER SONET-4-UPSR DSX-ALARM_DS1_LOS DSX-ALARM_DS1_LINK_DOWN DSX-ALARM_DS1_AIS DSX-ALARM_DS1_RAI DSX-ALARM_DS1_LOF DSX-ALARM_DS1_RX_LOMF DSX-ALARM_DS3_RX_RAI DSX-ALARM_DS3_TX_RAI DSX-ALARM_DS3_RX_AIS DSX-ALARM_DS3_TX_AIS DSX-ALARM_DS3_RX_LOF DSX-ALARM_DS3_RX_LOS DSX-ALARM_DS3_RX_IDLE DSX-ALARM_DS3_OTHER_FAILURE DSX-ALARM_DS3_LINK_DOWN DSX-ALARM_DS3_ADMIN_DOWN DSX-ALARM_DS1_OOF SDH-ALARM_DS3_TX_AIS SDH-ALARM_DS3_TX_AIS_Clear SDH-ALARM_DS3_RX_LOF SDH-ALARM_DS3_RX_LOF_Clear SDH-ALARM_DS3_RX_LOS SDH-ALARM_DS3_RX_LOS_Clear SDH-ALARM_DS3_OTHER_FAILURE SDH-ALARM_DS3_OTHER_FAILURE_Clear SDH-ALARM_DS3_RX_IDLE SDH-ALARM_DS3_RX_IDLE_Clear SDH-ALARM_LO_PAIS SDH-ALARM_LO_PAIS_Clear SDH-ALARM_LO_PLOP SDH-ALARM_LO_PLOP_Clear

Technology	Events
	SDH-ALARM_LO_PTIM SDH-ALARM_LO_PTIM_Clear SDH-ALARM_LO_PUNEQ SDH-ALARM_LO_PUNEQ_Clear SDH-ALARM_LO_PPLM SDH-ALARM_LO_PPLM_Clear SDH-ALARM_LO_PRDI SDH-ALARM_LO_PRDI_Clear SDH-ALARM_LO_BER_SD_B3 SDH-ALARM_LO_BER_SD_B3_Clear SDH-ALARM_LO_BER_SF_B3 SDH-ALARM_LO_BER_SF_B3_Clear SDH-ALARM_LO_LOM SDH-ALARM_LO_LOM_Clear SDH-ALARM_LO_PRFI SDH-ALARM_LO_PRFI_Clear SDH-ALARM_DS1_LOS SDH-ALARM_DS1_LOS_Clear SDH-ALARM_DS1_OOF SDH-ALARM_DS1_OOF_Clear SDH-ALARM_DS1_AIS SDH-ALARM_DS1_AIS_Clear SDH-ALARM_DS1_RAI SDH-ALARM_DS1_RAI_Clear SDH-ALARM_DS1_RX_LOMF SDH-ALARM_DS1_RX_LOMF_Clear SDH-ALARM_DS3_RX_AIS SDH-ALARM_DS3_RX_AIS_Clear SDH-ALARM_DS3_TX_RAI SDH-ALARM_DS3_TX_RAI_Clear SDH-ALARM_DS3_RX_RAI SDH-ALARM_DS3_RX_RAI_Clear SDH-ALARM_SONET_LINK_DOWN SDH-ALARM_SONET_LINK_DOWN_Clear SDH-ALARM_LRFI SDH-ALARM_LRFI_Clear SDH-ALARM_SONET_ADMIN_DOWN SDH-ALARM_SONET_ADMIN_DOWN_Clear SDH-ALARM_PRFI SDH-ALARM_PRFI_Clear SDH-ALARM_SLOS SDH-ALARM_SLOS_Clear SDH-ALARM_SLOF SDH-ALARM_SLOF_Clear SDH-ALARM_LAIS SDH-ALARM_LAIS_Clear SDH-ALARM_LRDI SDH-ALARM_LRDI_Clear SDH-ALARM_PAIS SDH-ALARM_PAIS_Clear SDH-ALARM_PLOP SDH-ALARM_PLOP_Clear SDH-ALARM_PUNEQ SDH-ALARM_PUNEQ_Clear SDH-ALARM_PPLM SDH-ALARM_PPLM_Clear SDH-ALARM_PRDI SDH-ALARM_PRDI_Clear SDH-ALARM_LOM SDH-ALARM_LOM_Clear SDH-ALARM_B1

Supported and Unsupported Events for Event Flow Controllers

Technology	Events
	SDH-ALARM_B1_Clear SDH-ALARM_B2 SDH-ALARM_B2_Clear SDH-ALARM_SF SDH-ALARM_SF_Clear SDH-ALARM_SD SDH-ALARM_SD_Clear
SyncE	ciscoNetsyncSelectedT0Clock ciscoNetsyncInputAlarmStatus ciscoNetsyncInputSignalFailureStatus NETCLK-6-SRC_ADD NETCLK-6-SRC_UPD NETCLK-6-SEL_CLOCK_SRC NETCLK-6-ENTER_HOLDOVER NETCLK-6-SRC_REM
VCOP	SSFP_VCOP-4-CONF_ADD SSFP_VCOP-4-CONF_DEL SSFP_VCOP-4-CONF_EXIST SSFP_VCOP-4-DEV_REM SSFP_VCOP-4-DEV_INS IOSXE_OIR-6-REMSSFP IOSXE_OIR-6-INSSSFP
Segment routing	OS-XTC-5-SR_POLICY_UPDOWN
Other (priority events)	SYS-5-RELOAD SYS-5-RESTART OIR-6-INSCARD OIR-SP-6-INSCARD SWT_CEFC_STATUS_CHANGE cefcFRURemoved cefcFRUInserted



APPENDIX G

Reference - Apache VTL Syntax

Reference - Apache VTL Syntax

Variable	Syntax	Output
Normal Variable	`#set($a = "ValueA")` `show $a`	`ValueA`
Array of integers	`#set($a = [1..3])` `show $a[2]`	`3`
Array of strings	`#set($a = ["ValueA", $ValueB, "ValueC"])` `show $a[2]`	`ValueC`
Map	`#set($a = {"ValueA" : "ValueB", "ValueC" : "ValueD"})` `show ${a.ValueA}`	`ValueB`

Reference - Apache VTL Syntax

INDEX