



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](#).

- [Web Client Requirements, on page 1](#)
- [Log In and Out, on page 2](#)
- [Setup Tasks to Complete Before Using Cisco EPN Manager, on page 2](#)
- [Change Your Password, on page 3](#)
- [Use the Main Window Controls, on page 3](#)
- [Change Your Default Home Page, on page 5](#)
- [Set Up and Use the Dashboards, on page 6](#)
- [Work In a Different Virtual Domain , on page 26](#)
- [Manage Jobs Using the Jobs Dashboard, on page 27](#)
- [Change User Preferences, on page 29](#)
- [Extend Cisco EPN Manager Functions, on page 30](#)
- [Check Cisco.com for the Latest Cisco EPN Manager Documentation, on page 31](#)

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 listed below.
- Browsers:
 - Google Chrome versions 44 to 76
 - Mozilla Firefox ESR 60
 - Mozilla Firefox versions 39 to 68
 - Microsoft Internet Explorer (IE) 11.0



Note Internet Explorer users have reported slower performance compared to other browsers, meaning that some GUI pages take longer to load in IE.

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

**Note**

A maximum of three Cisco EPN Manager tabs can be open simultaneously in a single browser session.

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

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 server's security certificate. 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 EPN Manager](#)—Describes all classes of users supported by Cisco EPN Manager, including the various CLI user accounts.
- [Types of User Groups](#)—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:
Set up and configure the Cisco EPN Manager server.	Server Setup Tasks
Add devices to Cisco EPN Manager and create device groups to simplify device and network management.	Add and Organize Devices
Enable monitoring for interfaces and technologies used by the network.	Monitor Device and Network Health and Performance
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

Change Your Password



You can change your password at any time by clicking  at the top right of the Cisco EPN Manager window and choosing **Change Password**. Click the ? (**help**) icon to review the password policy.

(Optional) Click the **Generate New Password** button to set a secured system-generated password. On clicking this button, a new password will be displayed in the adjacent text box. The same is also displayed in the **New Password** and **Confirm Password** text boxes. Click the eye icon in the text box to view or hide the password. You can also copy the password to clipboard by clicking the **Copy** button.

Click the **Reset** button to clear the values in the text box.


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 user name 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 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 26.



	Web GUI global settings button—Log out, change password, view your Cisco.com account profile, adjust your GUI preferences, check a Cisco.com support case, launch online help
---	---



When you click  on the right side of the title bar, the window settings menu opens.

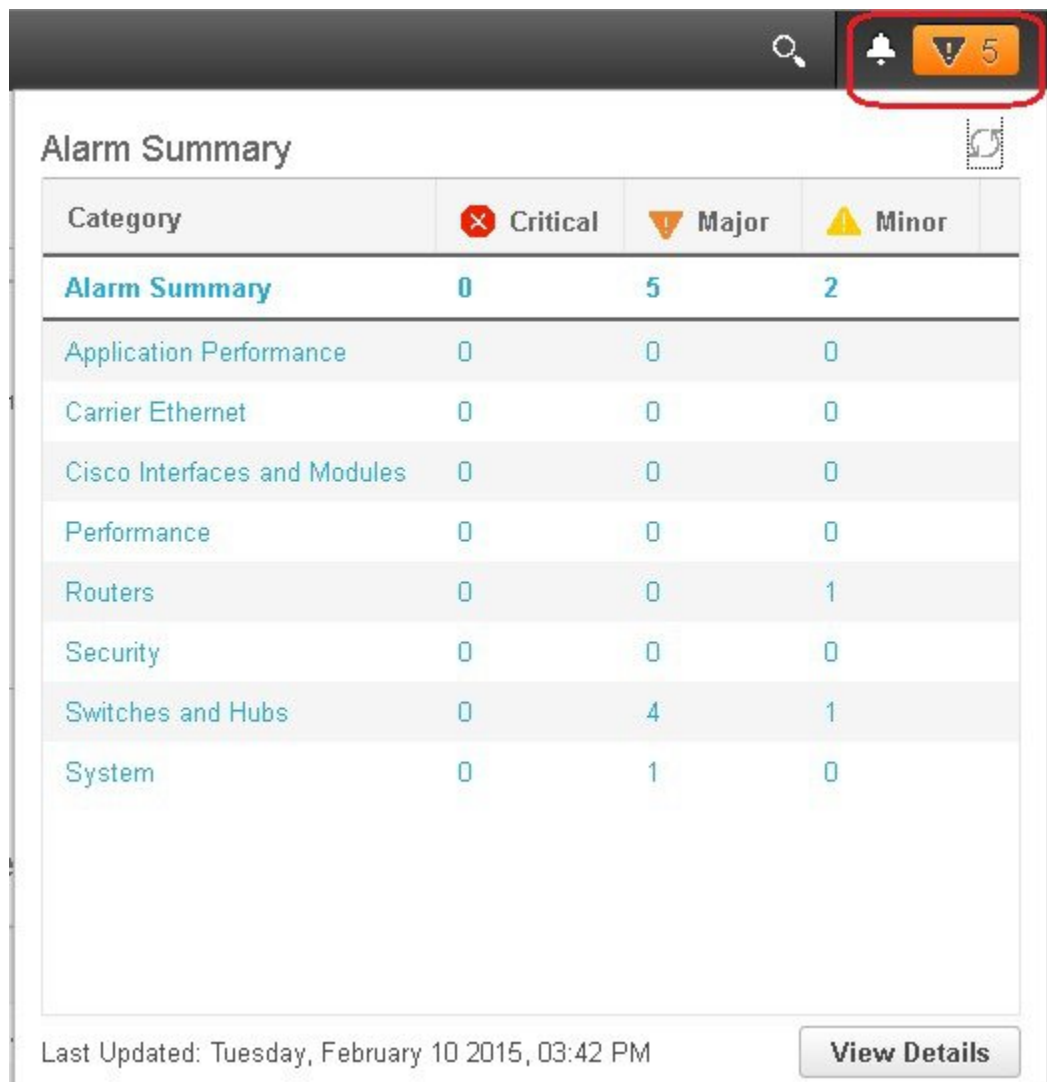
Figure 1: Window Settings






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

	<p>Alarm Summary—Provides a visual count of alarms in the categories you specify. Clicking this area opens the Alarm Summary popup window.</p>
---	---

When you click the **Alarm Summary** button (circled in the following figure), 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. In this example, the button displays a count for Switches and Hubs and System alarms, and the Alarm Summary pop-up to show all of the alarm categories listed in the following illustration.




Category	 Critical	 Major	 Minor
Alarm Summary	0	5	2
Application Performance	0	0	0
Carrier Ethernet	0	0	0
Cisco Interfaces and Modules	0	0	0
Performance	0	0	0
Routers	0	0	1
Security	0	0	0
Switches and Hubs	0	4	1
System	0	1	0


Last Updated: Tuesday, February 10 2015, 03:42 PM [View Details](#)

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 as well as 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 5](#).

Use the following dashboards to monitor and manage your network:

- **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](#).
- **Device Trends** dashboard—To view performance information for a specific device, application, or service. See [Device Trends 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](#).
- **Cable** dashboard —To view performance information for your cable network including the important issues currently affecting your network of Cisco cBR-8 devices. See [Cable Dashboard Overview, on page 15](#).

Users with administrator privileges can also use the following dashboards:

- **Licensing** dashboard—See [View the Licensing Dashboard](#).
- **Jobs** dashboard—See [Manage Jobs Using the Jobs Dashboard, on page 27](#).
- **System Monitoring** dashboard—See [Check Cisco EPN Manager Server Health, Jobs, Performance, and API Statistics Using the System Monitoring Dashboard](#).

Note the following:

- For an explanation of the parts of the dashboard window and how to use dashboard filters, see [How to Use the Dashboards, on page 20](#).
- 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	<p>For the selected Circuit Emulation (CEM) circuit:</p> <ul style="list-style-type: none"> • 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 re-ordered 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 <p>Note To view these dashlets, both the CEM and Pseudowire Emulation Edge to Edge monitoring policies must be enabled. See Monitoring Policies Reference.</p>
TE Tunnel	<p>For the selected Traffic Engineering (TE) tunnel circuit:</p> <ul style="list-style-type: none"> • 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	<p>For the selected circuit or VC:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Average traffic between endpoints • QoS class traffic and drops <p>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 post-policy data.</p> <ul style="list-style-type: none"> • 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	<p>Lists the circuits and VCs with the highest values for the following parameters:</p> <ul style="list-style-type: none"> • Delay • Jitter • Service loss • Traffic (both inbound and outbound) <p>You can toggle between the information for CE and L3VPN services.</p>

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring](#).
- 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 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
Interfaces	<p>For the selected interface:</p> <ul style="list-style-type: none"> • 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): <ul style="list-style-type: none"> • Traffic • Utilization • Errors • Discards • Cyclic redundancy check (CRC) errors <p>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).</p> <ul style="list-style-type: none"> • 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 pre-policy rate, post-policy rate, and drops percentage) • QoS class map policy statistics (inbound and outbound)
QoS	<p>For the selected QoS policy:</p> <ul style="list-style-type: none"> • Summary information • Statistics and graphs for pre-policy, post-policy, and dropped class map traffic • Statistics and graphs for conforming, exceeding, and violating class map traffic

Dashboard Tab	Information Provided
Y1731	<p>For Layer 2 services on the selected probe:</p> <ul style="list-style-type: none"> • Summary information • ITU-T Y.1731 statistics • Delay, jitter, and frame loss, CCM frame loss between endpoints • Jitter Bins Statistics • Delay Bins Statistics • Endpoint availability
IP SLA	<p>For Layer 3 services on the selected probe:</p> <ul style="list-style-type: none"> • Summary information • IP Service Level Agreement (SLA) statistics • Delay, jitter, and frame loss between endpoints • Endpoint availability
BNG Statistics	<p>Broadband Network Gateway (BNG) information for the selected device:</p> <ul style="list-style-type: none"> • Details such as its name, IP address, product type, and software version • Names of configured IP pools, as well as 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 <p>Note the following:</p> <ul style="list-style-type: none"> • Use the check boxes below the charts to select the items you want to view information for • 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	<p>Quality of Service (QoS) information for the selected service on a Cisco ME 1200 device:</p> <ul style="list-style-type: none"> • 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. <p>Note the following:</p> <ul style="list-style-type: none"> • Five traffic graphs are provided: one for each traffic type as well as 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.
Optical SFPs	<p>For the selected Small Form-Factor Pluggable (SFP) Transceiver Module interface:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Optical input and output power • Operating temperature • Transceiver supply voltage • Laser bias current • Individual graphs that chart the operating metrics listed in the SFP Statistics dashlet

Dashboard Tab	Information Provided
SONET/TDM Interfaces	<p>For the selected SONET or time-division multiplexing (TDM) interface:</p> <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Errored seconds • Severely errored seconds • C-bit severely errored seconds • P-bit severely errored seconds • Unavailable seconds <p>Values are provided for both the near-end (the receiving end) and far-end (the transmitting end) of the interface</p> <ul style="list-style-type: none"> • Individual graphs that chart the performance metrics listed in the SONET/TDM Statistics dashlet
Device Sensors	<p>For the sensors that reside on the selected device, details such as their name, the type of information they collect (such as temperature or voltage) and the corresponding unit of measure, and the value recorded during the last device poll.</p> <p>Note Sensor data is not polled by default. To enable the collection of this data, create a monitoring policy based on the Device Sensors policy type (see Create a New Monitoring Policy Using Out-of-the-Box Policy Types).</p>
MPLS Links	<p>You can get the following details for the link you select:</p> <ul style="list-style-type: none"> • Link details such as the link name, endpoint device and interface. • Link delay (one-way and two-way). <p>Note You can click Link Name in the Top N MPLS Links Table to launch the MPLS links dashboard on the selected link.</p>

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring](#).
- 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	<ul style="list-style-type: none"> Status (ICMP reachability, SNMP reachability, device manageability), system health, and alarm summary metric dashlets <p>Note the following:</p> <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> Top N devices by CPU utilization, memory utilization, and environmental temperature <p>For the Top N Environmental Temperature dashlet, note the following:</p> <ul style="list-style-type: none"> 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. <ul style="list-style-type: none"> Network topology

Dashboard Tab	Information Provided
Incidents	<ul style="list-style-type: none"> • System health and alarm summary metric dashlets <p>Note the following:</p> <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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	<p>For the selected port group:</p> <ul style="list-style-type: none"> • Interface availability and utilization summaries • Top N devices by interface traffic, errors and discards, cyclic redundancy check (CRC) errors, and utilization <p>Note the following:</p> <ul style="list-style-type: none"> • 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). • Due to a limitation in the current release, the Interface Health monitoring policy polls all of the interfaces in your network for CRC error data, not just the ones associated with the port group you chose from the Port Groups drop-down list. Keep this in mind when you view the data provided by the Top N Interface CRC Errors dashlet. • Bottom N devices by interface availability <p>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>i</i> (information) icon.</p>

Dashboard Tab	Information Provided
Top N QoS	<p>For the selected port group:</p> <ul style="list-style-type: none"> • Top N devices by QoS pre-policy, post-policy, and drop rates • Top N devices by conforming, exceeding, and violating traffic rates <p>You can toggle between inbound and outbound traffic data.</p>
Top N Y1731	<p>Endpoints with the highest values for the following parameters:</p> <ul style="list-style-type: none"> • Delay (one- and two-way) • Jitter (one-way) • Frame loss
Top N MPLS Links	<ul style="list-style-type: none"> • Delay (one-way and two-way) <p>Note You can click Link Name in the Top N MPLS Links Table to launch the MPLS links dashboard on the selected link.</p>

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).
- 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 EPN Manager Is Monitoring](#).
- For a description of how to customize the contents and layout of a dashboard tab, see [Customize a Dashboard Tab](#).

Cable Dashboard Overview

The **Cable** dashboard provides an executive overview of your cable network including the important issues currently affecting your network of Cisco cBR-8 devices. To open this dashboard, choose **Dashboard > Cable > cBR-8 Dashboard**.

Since Cable dashboards can provide both a high level overview and detailed insights of the cable network, dashboards are equipped with filter conditions that help in refining the displayed information.

- Filter information based on location or capabilities. The location you choose could be the group or location to which multiple devices are assigned.
- Filter information associated with a specific Cisco cBR-8 device.
- In addition to the above filters, the dashlets are interactive and can refine data further based on your need:
 - To refine the information provided in the table, you can do two things: First, you can create and apply a filter. And second, you can click a particular graph element. For example, in the **cBR-8 Dashboard** tab, if you click the bar that corresponds to a Cisco IOS XE version in the **Software Version** bar graph, the **Software Version Details** table only displays the information specific to that version.
 - Filters applied within a tab are applicable to all dashlets within the tab. For example, in the **Cable Modem** tab, if you filter a specific Cisco cBR-8 device, then all dashlets (such as **Modem Count by Vendors** and **Modem Count by Capability**) display information associated only with the filtered Cisco cBR-8 device.

The information provided in these tabs is refreshed periodically and can be configured through cable policies. To export the details displayed in the table rows as a .csv file, use the **Export** button.

Before you begin:

To ensure that information is collected and reported for the Cisco cBR-8 routers in your network, verify that **Cable Policies** is listed on the **Monitoring Policies** page (**Monitor > Monitoring Tools > Monitoring Policies > Policies** pane), is currently active, and has polling intervals set for its parameters. To activate Cable monitoring policies, see, [Change Thresholds and Alarm Behavior for a Monitoring Policy](#).

Dashboard Tab	Information Provided
cBR-8 Dashboard	<p>Provides interactive graphs that chart the following metrics for the Cisco Converged Broadband Router-8 (cBR-8) routers in your network:</p> <ul style="list-style-type: none"> • Software version—Indicates the number of routers (Cisco cBR-8 devices) running various Cisco IOS XE versions. • License usage—Indicates the number of license types applied to the selected routers. • License state—Indicates the number of routers with registered or unregistered licenses. • High availability (HA)—Indicates the number of routers configured with stateful switchover (SSO). • Remote physical device—Indicates the number of RPDs that are currently online, offline, being initialized with Cisco cBR-8 devices, in 'defined' state, or for whom deployment is pending. <p>Note</p> <ul style="list-style-type: none"> • Device statistics in the dashboard is available only for the RPDs associated with Cisco cBR-8 devices. • RPD Polling information is displayed in the Cable dashboard, and it can be dynamically changed by the user by editing the property file. For more information, see RPD Polling. • Supervisor FPGA Versions—Indicates the field programmable gate arrays (FPGAs) currently in use, broken down by type and version. <p>To view a table that provides additional information for one of these metrics, place your cursor over a metric and click anywhere within the resulting box that appears. For example, open the High Availability Details table and it provides information such as the name and IP address of Cisco cBR-8 routers, the amount of time they have been up, and the location of associated active and standby HA servers.</p> <p>You can also open a device's 360 view (Device 360, RPD 360, and Interface 360) by clicking the relevant <i>i</i> (information) icons displayed in the device details columns.</p>

Dashboard Tab	Information Provided
Cable Alarm	<p>Using interactive graphs for the alarms raised on Cisco cBR-8 routers in your network, the Alarm dashboard provides various statistics such as:</p> <ul style="list-style-type: none"> • Alarm Severity: Indicates the number of alarms with different severity levels (Critical, Major, Minor, Warning, and Cleared). • Alarm Category: Indicates the number of alarms with a particular alarm category (such as CMTS System, CMTS Subscriber, Broadband Cable, etc.). • Group Location of Devices: Indicates the number of alarms raised on devices belonging to specific groups. • cBR-8 Name: Group alarms raised on a specific cBR-8 device. <p>You can filter alarms to view additional details about the alarm such as the alarm ID, failure source, time when the alarm was raised, the alarm protocol category, condition, and whether the alarm affects services. For more information about the alarm, use the Alarm ID hyperlink to navigate to the Alarms and Events page.</p> <p>In addition to various filters, the alarm heatmap provides a comprehensive count of alarms from various geographic locations and cBR-8 devices. The data is periodically refreshed and also updated based on your selection of the group location, device, or alarm severity.</p> <p>In case of certain hardware alarms, user can navigate from the Alarms and Events page to the chassis view of the associated cBR-8 platform by performing the steps below:</p> <ol style="list-style-type: none"> 1. In the Alarms and Events page, under the Failure Source column, click on the <i>i</i> icon next to relevant event to open the Device 360 page. 2. In the Device 360 page, click View > Chassis View to open the chassis view of the selected cBR-8 device. The failed module within the cBR-8 platform will be highlighted in the chassis view. <p>Note Few sample alarm conditions that can be investigated by the user for a cBR-8 device are:</p> <ul style="list-style-type: none"> • cefcFruRemoved (when power supply and/or fan is removed) • cefcPowerStatusChange (when power supply becomes faulty) • cefcFanStatusChange (when fan becomes faulty)

Dashboard Tab	Information Provided
Cable Modem	<p>Provides interactive graphs that chart the following metrics for cable modems associated with Cisco cBR-8 routers in your network:</p> <ul style="list-style-type: none"> • Cable Modem—Indicates the total count and operational states (such as Online, Offline, and Initialization) of available modems. • Modem Count by Vendors—Indicates the total number of online/offline cable modems from various vendors (such as Cisco, Aris), by mapping the MAC address in the cable modem to the corresponding vendor name and vendor count. • Modem Count by Capability—Indicates the total number of online or offline cable modems with various DOCSIS versions (such as DOCSIS 2.0, DOCSIS 3.1, etc.). <p>Note If you choose All (devices) in the filter option, only those devices associated with cable modems are filtered. The dashlets do not represent information about cable devices with no cable modems.</p> <ul style="list-style-type: none"> • Flap Count—Provides the consolidated view of the flapping modems. Click the flap count hyperlink in the underlying table to open the Flap Details tab.

For a description of how to customize the contents and layout of a dashboard tab, see [Customize a Dashboard Tab](#).

Device Trends Dashboard Overview

From the **Device Trends** dashboard, you can view performance information for a specific device, application, or service. To open this dashboard, choose **Dashboard > Device Trends >** any of the tabs described in the following table.

Dashboard Tab	Information Provided
Device	<p>For the selected device:</p> <ul style="list-style-type: none"> • CPU utilization and memory utilization • Health information • Port summary
Application	<p>For the selected application or service:</p> <ul style="list-style-type: none"> • Traffic rate and volume • Top N clients, servers, and applications by traffic rate and volume

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring](#).
- For a description of how to customize the contents and layout of a dashboard tab, see [Customize a Dashboard Tab](#).

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 physical, Optical Data Unit (ODU), Optical Transport Unit (OTU), Ethernet, Synchronous Optical Network (SONET), and Synchronous Digital Hierarchy (SDH) interfaces. The performance information is presented in different tabs per interface type.

To open this dashboard, do one of the following:

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

Note the following:

- Interface monitoring is not enabled by default. For information on how to check this, see [Check What Cisco EPN Manager Is Monitoring](#).
- 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 you can use to adjust them.

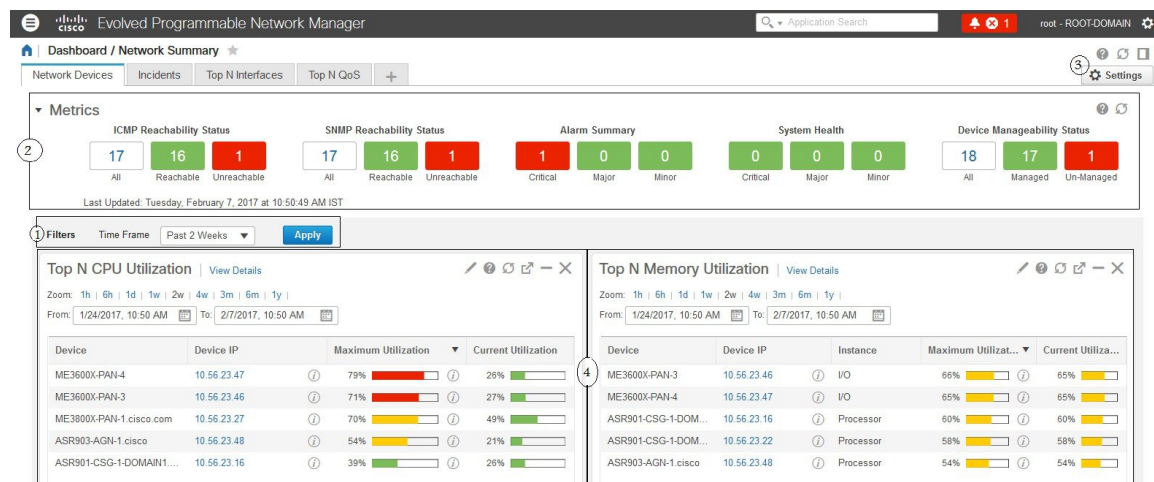
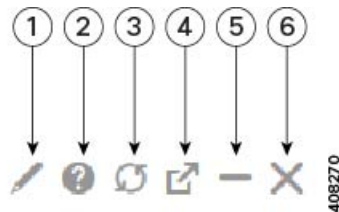


Table 2: Dashboard Elements

1	Dashboards 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.

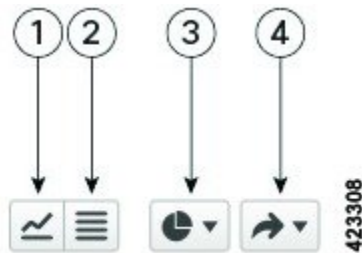
3	<p>Dashboard settings and controls:</p> <ul style="list-style-type: none"> • Dashboard icons—Allows you to launch online help, refresh the entire dashboard, and open the Dock window. • Dashboard Settings menu—Allows you to add or rename a dashboard tab, add new dashlets (both standard and metric), adjust the dashboard's layout, reset all dashboards to their default settings, and export data from the selected dashlets. <p>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.</p>
4	Standard dashlets—Provides at-a-glance data that is relevant to the dashboard.

In the top right corner of each dashlet are 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 needs to be activated in order for the dashlet to collect data, and lists the filters that can be applied to the dashlet.
3	Refresh icon—Click to refresh the information displayed in the dashlet.
4	Detach icon—Click to move the dashlet to another location in the dashboard.
5	Collapse/Expand icon—Click to toggle between a maximized and minimized dashlet.
6	Close icon—Click to remove the dashlet from the dashboard.

In the bottom right corner of dashlets that provide charts, you can find the buttons highlighted in the following figure. The buttons that are available will vary among dashlets.



1	Chart View button—Click to view a dashlet's information as a chart.
---	--

2	Table View button—Click to view a dashlet's information as a table.
3	Chart Type button—Click to choose the type of chart a dashlet displays (such as a bar or pie chart) and any options you want to set (such as displaying a unique fill pattern for each element).
4	Actions button—Click to print the information provided by a dashlet or export the information as either a .csv or .pdf format file.

See these topics for additional information on dashboards:

- [Types of Dashboards, on page 6](#)
- [Add Dashlets to Dashboards, on page 23](#)
- [Add a New Dashboard, on page 22](#)
- [Find Out Why Data Is Missing from a Dashboard](#)

Add a New Dashboard

Use this procedure to create a new dashboard. Your new dashboard will appear as a new tab under one of the dashboards listed in [Types of Dashboards, on page 6](#).

-
- 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 + (**Add New Dashboard**) tab.
- The **Settings** menu opens.
- Step 3** Enter a name for the new dashboard, then click **Apply**.
- Step 4** Click the new dashboard tab, then add dashlets as described in [Add a Predefined Dashlet To a Dashboard, on page 23](#).
-

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 **Dashboard >** the dashboard tab you want to customize.
- For example, if you want to customize the **Performance** dashboard's **BNG** tab, choose **Dashboard > Performance > BNG**.
- Step 2** Adjust the dashboard tab as needed.
- You can do things like:
- 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 23](#).
- Customized dashlets that you create to monitor device performance—These dashlet types can only be added to the **Device Trends** dashboard. See [Add a Customized Dashlet to the Device Trends Dashboard](#).

Add a Predefined Dashlet To a Dashboard

Cisco EPN Manager provides a predefined set of dashlets that will provide 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](#).)

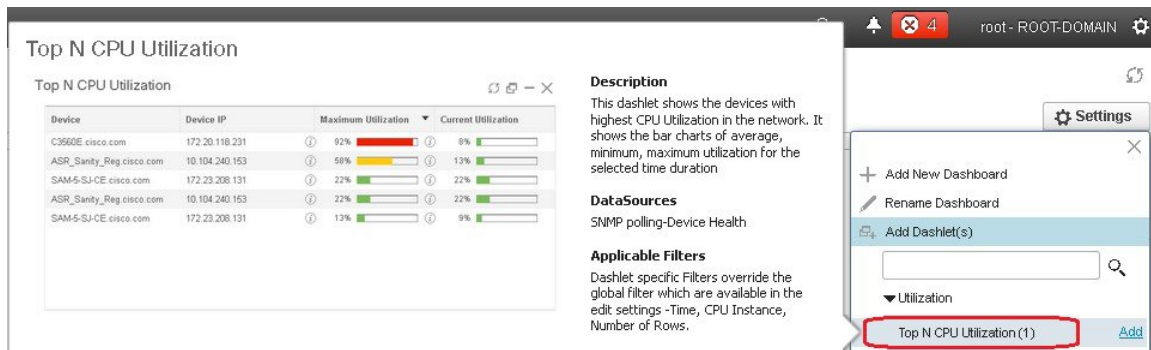
Step 1 From the sidebar menu, choose **Dashboard**, then select the dashboard you want to add a dashlet to.

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

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

- 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.
- 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 the dashlet provides and the filters you can apply to the dashlet, as shown in the following illustration.

Add a Customized Dashlet to the Device Trends Dashboard



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.)

- From the top right corner of the dashlet, click its ? (**Help**) icon to open the dashlet's pop-up window.
- 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 EPN Manager Is Monitoring](#).

Add a Customized Dashlet to the Device Trends Dashboard

If none of the dashlets in the **Device Trends** dashboard provide the device performance information you need, you can add a dashlet that uses a customized template to poll devices for their SNMP MIB attributes. Complete the following procedure to add this dashlet to the dashboard.

Before you begin

Check the available monitoring policies to determine which policy collects the information you need. You will have to specify a policy during the dashlet creation process. If none of the policies meet your needs, you can create a policy that polls new parameters. See [Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices](#).

Step 1 Choose **Dashboard > Device Trends > Device**.

Step 2 From the top right corner of the dashboard, click **Settings** and then click **Add Dashlet(s)**.

Step 3 Expand the **Device Dashlets** list.

Step 4 Locate **Generic Dashlet**, then click **Add**.

Cisco EPN Manager adds a blank generic dashlet to the **Device Trends** dashboard.

Step 5 Configure the new dashlet as needed.

At a minimum, you should:

- Enter a meaningful title in the **Dashlet Title** field.
- Check the **Override Dashboard Time Filter** check box if you do not want to apply the time filters to all of the dashlets in the dashboard.
- In the **Type** drop-down list, choose whether the dashlet will display its data as a table or line chart. (Regardless of your choice, Cisco EPN Manager will display a toggle at the bottom of the dashlet that allows you to change the format.)
- In the **Policy Name** drop-down list, choose the monitoring policy that will collect the data for this dashlet. See [Monitoring Policies Reference](#) for descriptions of the available monitoring policies.

Step 6 Click **Save And Close**.

If no data is displayed in the dashlet, see [Find Out Why Data Is Missing from a Dashboard](#).

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**):

- Open the web GUI page you want to add.
- 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**):

- 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, 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](#).

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

See [Find Devices With Inventory Collection or Discovery Problems](#).

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](#).

- 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](#). 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](#).

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


See [How Data Retention Settings Affect Web GUI Data](#).

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 administrator 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](#).

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. If this is the case, 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 .

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.

Button	Description
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.

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 jobs that triggers.
- 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	<p>Use this setting to define the number of entries displayed on the Monitoring pages for APs, Controllers, Site Maps, Roles & AAA > Active Sessions.</p> <p>By default, 50 entries are listed.</p> <p>Note This setting does not apply to Network Devices, Alarms and Events, configuration archive, software image management, or configuration.</p>
Maps	Use Next Generation Maps	By default, this setting is enabled.
Network Topology	Automatically switch device group selection to show all participating devices	By default, this setting is not enabled.
	Refresh Interval for Maps and Tables	<p>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 Do not refresh if you do not want to refresh the maps and tables.</p> <p>By default, the refresh interval is 1 minute.</p>
Chassis View Configuration	UI Rrefresh Interval	<p>Use this setting to define how often the data in the UI is refreshed in the chassis view.</p> <p>By default, the UI refresh interval is 1 minute.</p>
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 10 mins. 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.

For information about user preference settings in Alarms and Events, see [Set Up Your Alarm and Event Display Preferences](#).

Extend Cisco EPN Manager Functions

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

- Cisco Evolved Programmable Network Manager MTOSI API—Integrates Cisco EPN Manager with your Operations Support System (OSS).
- Cisco Evolved Programmable Network 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](#)



Note

MTOSI NBI is being deprecated and is disabled by default. To enable MTOSI NBI, see the [Cisco Evolved Programmable Network Manager MTOSI API Guide for OSS Integration](#).

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.
