



## Monitor Device and Network Health and Performance

---

- [How Device Health and Performance Is Monitored: Monitoring Policies](#)
- [Set Up Interface Monitoring](#)
- [Use the Dashboards To Check Network and Device Health](#)
- [Check What Cisco EPN Manager Is Monitoring](#)
- [Check a Monitoring Policy's Device, Polling, Threshold, and Alarm Settings](#)
- [Check the Status of Past Data Collections](#)
- [Monitor New Information By Creating a New Monitoring Policy](#)
- [Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices](#)
- [Change the Device Set a Policy is Monitoring](#)
- [Change the Polling Interval for a Monitoring Policy](#)
- [Change Thresholds and Alarm Behavior for a Monitoring Policy](#)
- [Run Performance Tests](#)

### How Device Health and Performance Is Monitored: Monitoring Policies

*Monitoring policies* control how Cisco EPN Manager monitors your network by controlling the following:

- What is monitored—The network and device attributes Cisco EPN 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 should Cisco EPN Manager 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 EPN Manager. Monitoring policies do not make any changes on devices.

## LIMITED ORDERABILITY RELEASE

These steps summarize how you can configure a monitoring policy.

1. Identify the NE elements you want to monitor.
2. Create (add) a new monitoring policy using a supported monitoring *policy types* (these are summarized in [Table 7-1](#)).
3. Customize the policy. Depending on the policy, your customizations can include adjusting polling frequencies, specifying thresholds, and indicating whether Cisco EPN Manager should generate an alarm when the threshold is surpassed. You can also specify the alarm severity.
4. Choose the devices that the policy should monitor (Cisco EPN Manager filters out any devices to which the policy does not apply).
5. Activate the policy.

To view and administer monitoring policies, choose **Monitor > Monitoring Policies**. Policies are generally listed under:

Navigation	Description
<b>Monitor &gt; Monitoring Policies &gt; Automonitoring</b>	Lists the policies that are enabled by default in Cisco EPN Manager. When you choose a policy from <b>Automonitoring</b> , the policy is in <i>edit</i> mode. By default, only the Device Health policy is enabled by default. It monitors general device health (CPU and memory utilization, operational status, and so forth).
<b>Monitor &gt; Monitoring Policies &gt; My Policies</b>	Lists all policies that the user created or has permission to view. When you choose a policy from <b>My Policies</b> , the policy is in <i>view</i> mode. To edit the policy, choose it and click <b>Edit</b> .



### Note

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 [Table 7-1](#).

Note that interface monitoring is *not* enabled by default. This is because for deployments with many configured interfaces, monitoring all interfaces could negatively impact system performance. To enable interface monitoring, see [Set Up Interface Monitoring](#).

Cisco EPN Manager provides out-of-the-box policy templates called policy types. Policy types have predefined sets of attributes and settings that are tailored to the entity being monitored—for example, optical devices, Quality of Service (QoS), Ethernet OAM, and others. All you have to do is apply devices to a policy and enable it. You can create as many policies as you need using the same policy types, and then customize the settings in each policy. [Table 7-1](#) summarizes the policy types provided by Cisco EPN Manager. The table also directs you to where you can get more details about each policy.

**LIMITED ORDERABILITY RELEASE****Table 7-1 Supported Monitoring Policy Types**

Category	Policy Type	Description	For Policy Type Details, see:
Basic	Device Health	Monitors general device health: CPU utilization, memory pool utilization, environment temperature, and device availability. Supports customizing TCAs for utilization and temperature.  <b>Note</b> For Cisco NCS 2000 series and Cisco ONS devices, use the optical monitoring policies for device health monitoring.	<a href="#">Reference—Basic Monitoring Policies, page C-1</a>
	Interface Health	Monitors interface operational status and statistics (such as inbound/outbound errors, discards, utilization, and drops in queues) and interface performance (traffic, speed, and rate). Supports customizing TCAs for some attributes.  <b>Note</b> For optical interfaces (Cisco NCS 2000, Cisco 4000, and Cisco ONS devices), use the optical monitoring policies.	
	Custom MIB Polling	Monitors parameters that are not covered by any of the default policies provided by Cisco EPN Manager.  <b>Note</b> Use this policy to monitor attributes that are not included in any existing policy types. This allows you to extend Cisco EPN Manager monitoring abilities.	
Carrier Ethernet	Quality of Service	Monitors QoS and supports customizing TCAs for some attributes.	<a href="#">Reference—Carrier Ethernet Monitoring Policies, page C-2</a>
	IP SLA Y.1731	Monitors Metro Ethernet network using IP SLA Y.1731. Supports customizing TCAs for some attributes.	
	Pseudowire Emulation Edge to Edge	Monitors PWE3 networks. Supports customizing TCAs for some attributes.	
	Ethernet OAM	Monitors CFM-enabled networks using IP SLA Ethernet OAM. Supports customizing TCAs for some attributes.	
Optical	Optical 1 day	Monitors optical devices according to the default time period used by the policy. These policies monitor: <ul style="list-style-type: none"> <li>NCS 2000 and Cisco ONS devices—Basic device health monitoring and DWDM interfaces</li> <li>NCS 4000 devices—SONET/SDH, Physical, OTN (for general device health, use the Device Health monitoring policy)</li> </ul>	<a href="#">Reference—Optical Monitoring Policies</a>
	Optical 15 mins		

**LIMITED ORDERABILITY RELEASE**

## Adjust the Device Health Monitoring Policy

The Device Health monitoring policy is enabled by default. It checks managed devices for CPU utilization, memory pool utilization, environment temperature, and device availability. 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 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 [Monitor New Information By Creating a New Monitoring Policy, page 7-9](#).

## Set Up Interface Monitoring

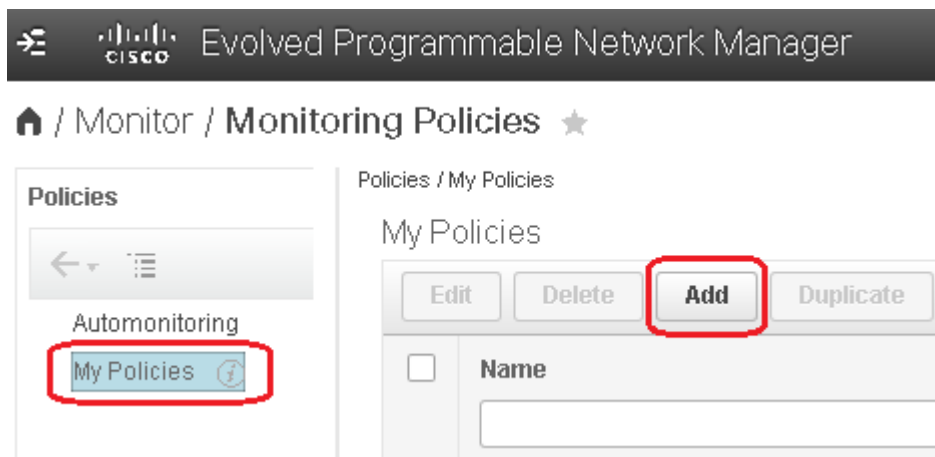
Interfaces are not monitored by default. This protects system performance for networks with large numbers of interfaces. To enable interface monitoring, create a new monitoring policy as described in the following procedure.

**Note**

The Interface Health monitoring policy does not collect data for Cisco NCS or Cisco ONS devices. You must use one of the optical policy types (see [Table 7-1](#)).

To set up and enable interface monitoring:

- Step 1** Choose **Monitor > Monitoring Policies**, then select **My Policies** from the list on the left.
- Step 2** Click **Add** to create a new policy.



- Step 3** Select a policy type—for example:
- Interface Health for generic interface monitoring
  - Optical 15 Mins to monitor DWDM interfaces on NCS 2000 and Cisco ONS devices

## LIMITED ORDERABILITY RELEASE

When you select a policy, Cisco EPN Manager populates the right side of the window with the policy settings.

- Step 4** Enter a meaningful name and description (this is an important step if your deployment will have many policies).
- Step 5** From the **Device Selection** drop-down list, select the devices (or device groups) to which you want to apply the policy. (Cisco EPN Manager only lists devices applicable to that policy.)  
If you want to use the default settings for polling and thresholds, proceed to [Step 8](#).
- Step 6** To adjust the polling interval, select a value from the **Polling Frequency** drop-down list. A policy may have one interval for all parameters, or per-parameter intervals.

For example, the following shows a policy that will monitor Cisco ASR 9000 interfaces. It uses the Interface Health policy type, where all parameters are polled using the same interval.

Policy Types / **Interface Health**

\* Device Selection ▼

\* **Name** ASR9K-IF-test **Author** root

**Description**  **Contact**

**Feature Category** Interface Health

---

### Parameters and Thresholds

Parameter	Condition
<input type="text"/>	
▶ Inbound Discards	
▶ Outbound Discards	
▶ Inbound Errors	
▶ Outbound Errors	
▶ Input Utilization	
▶ Output Utilization	
▶ Inbound bytes rate	

Polling Frequency: 1 min ▼  
 1 min  
 5 min  
 15 min  
 30 min  
 1 hour  
 6 hour  
 12 hour

▼

## LIMITED ORDERABILITY RELEASE

Alternatively, the following shows a policy that will monitor Cisco NCS 2000 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. (For information on the specific attributes that are polled by this policy—for example, the OTN attributes, Ethernet attributes, and so forth—see [Reference—Optical Monitoring Policies](#).)

Policy Types / **Optical 15 mins**

\* Device Selection

\* Name  Author root

Description  Contact

Feature Category Optical 15 mins

---

### Parameters and Thresholds

Parameter	Polling Fre...
<input type="text"/>	
Physical	15 min
<b>OTN</b>	15 min ▼
Ethernet	15 min
SonetSdh	15 min
Dwdm Infrastructure	15 min

**Step 7** If the policy supports TCA customization, you can adjust the thresholds. See [Change Thresholds and Alarm Behavior for a Monitoring Policy](#).

**Step 8** Click:

- **Save and Activate** to start monitoring immediately
- **Save and Close** to save the policy and activate it at a later time

Depending on the policy type and how your dashboards are set up, Cisco EPN Manager displays the monitored information in the dashboards. If a policy's information cannot be viewed from a dashboard, you can gather your data by running a report (see [Create, Schedule, and Run a New Report](#)). For information on dashboards, see [Set Up and Use the Dashboards](#).

**LIMITED ORDERABILITY RELEASE**

## Use the Dashboards To Check Network and Device Health

Cisco EPN Manager provides three dashboard types: the Overview dashboard, Network Summary dashboard, and Performance dashboard. The following table describes each dashboard and the type of information it can provide.

<b>If you want: performance information:</b>	<b>Choose Dashboards &gt; ...</b>	<b>Examples of what the dashboard provides:</b>
Across the network	<b>Overview</b>	<ul style="list-style-type: none"> <li>Statistics for unreachable devices</li> <li>Statistics for operationally up and down interfaces</li> <li>Software images being used with device counts for each</li> <li>Most recent alarms in the network</li> </ul>
Tabulated per devices and interfaces	<b>Network Summary</b>	<ul style="list-style-type: none"> <li>Alarms that are occurring most frequently</li> <li>Devices with the highest memory utilization, CPU utilization, environmental temperatures</li> <li>Interfaces with the highest utilization</li> </ul>
For a specific device	<b>Performance</b>	<ul style="list-style-type: none"> <li>Device alarms</li> <li>Device temperature</li> <li>Device reachability history</li> <li>Device CPU and memory utilization</li> <li>Interface availability, discards, utilization, and QoS for a specific device interface on the device</li> </ul>

To adjust what is displayed on your dashboards, see:

- [Set Up and Use the Dashboards](#)
- [Add a New Dashlet To An Existing Dashboard](#)

## Check What Cisco EPN Manager Is Monitoring

To view what is currently being monitored by Cisco EPN Manager, choose **Monitor > Monitoring Policies > My Policies**. Cisco EPN Manager lists the monitoring policies you created or have access to, with their status and details, as shown in the following table.

<b>Policy Field</b>	<b>Description</b>
Type	Template (policy type) used to create this policy. The policy types are listed in <a href="#">Table 7-1</a> .
Status	Active or Inactive. A policy can be inactive if it was created but never activated (the <b>Save and Activate</b> button was never clicked).
Threshold	Whether the policy monitors any parameter thresholds.
Activation History	Hyperlink to a table listing the time of activation and devices monitored
Collection Status	Hyperlink to a table listing the data that was collected

## LIMITED ORDERABILITY RELEASE

To get details about a specific policy, choose **Monitor > Monitoring Policies > My Policies** and select a policy from the list on the left. Depending on the policy type, the following information is displayed when you choose a policy.

Policy Field	Description
General Information	Name, description, creator, status, policy type (Feature Category).
Device Selection	Devices which the policy is monitoring.
Polling Frequency	How often Cisco EPN Manager polls the device parameters.
Parameters and Thresholds	Which parameters are polled. If any thresholds or alarms are associated with a parameter, they are listed next to it.

## 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 Policies > 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.
  - 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.  
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.  
Optical policy thresholds cannot be customized.
- 

For information on changing these settings, see:

- [Change the Device Set a Policy is Monitoring](#)
- [Change the Polling Interval for a Monitoring Policy](#)
- [Change Thresholds and Alarm Behavior for a Monitoring Policy](#)

## Check the Status of Past Data Collections

To check the status of past data collections:

- 
- Step 1** Choose **Monitor > Monitoring Policies > My Policies**.
  - Step 2** Locate the policy, and under the Collection Status, click **Details** to open the Collection Data dialog.
-



**LIMITED ORDERABILITY RELEASE**

# Monitor New Information By Creating a New Monitoring Policy

The following procedure explains how to create a new monitoring policy. You can create a new policy in two ways:

- [Create a New Monitoring Policy Using Policy Types](#)
- [Create a New Monitoring Policy Based On An Existing Policy](#)

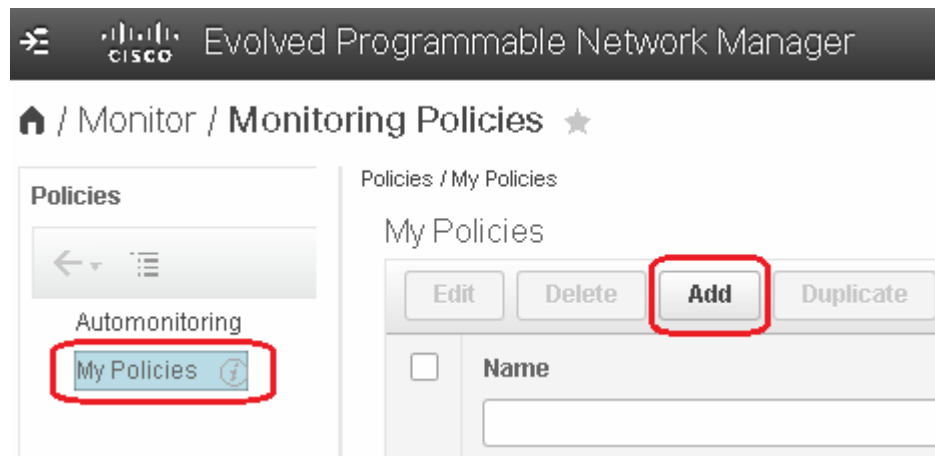
To edit an existing policy, see:

- [Change the Device Set a Policy is Monitoring](#)
- [Change the Polling Interval for a Monitoring Policy](#)
- [Change Thresholds and Alarm Behavior for a Monitoring Policy](#)

## Create a New Monitoring Policy Using Policy Types

**Step 1** Check what is currently being monitored. See [Check What Cisco EPN Manager Is Monitoring](#).

**Step 2** Choose **Monitor > Monitoring Policies**, then click **Add**.



**Step 3** Select the policy type template you want to use from the Policy Types menu. To check which policies can be applied to port groups, see [Check What Cisco EPN Manager Is Monitoring](#).

**Step 4** Configure the new policy:

- 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.)
- Enter a name and contact, and edit the description.
- Under Parameters and Thresholds, configure the polling settings, parameter values, and alarm conditions. See [Change the Polling Interval for a Monitoring Policy](#) and [Change Thresholds and Alarm Behavior for a Monitoring Policy](#).

## LIMITED ORDERABILITY RELEASE

- 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 New Monitoring Policy Based On An Existing Policy

- Step 1** Check what is currently being monitored. See [Check What Cisco EPN Manager Is Monitoring](#).
- Step 2** Create the duplicate.
- Choose **Monitor > Monitoring Policies > My Policies**.
  - Locate the policy you want to duplicate.
  - Check the policy, then click **Duplicate**.
  - In the Duplicate Policy Creation dialog, choose the parent folder, enter a policy name and description, and click **OK**.
- Step 3** Make your changes to the duplicate.
- Locate the policy under My Policies.
  - Check the policy and click **Edit**.
  - Make your changes as needed. See:
    - [Change the Device Set a Policy is Monitoring](#)
    - [Change the Polling Interval for a Monitoring Policy](#)
    - [Change Thresholds and Alarm Behavior for a Monitoring Policy](#)
- Step 4** 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.

## LIMITED ORDERABILITY RELEASE

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 Policies**, then 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 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 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.
- Step 7** To view the MIB polling data, create a generic dashlet using the name of the policy that you created (see [Create a Generic Dashlet to Monitor Performance Information](#)).



### Note

To view the SNMP polling data for Cisco ASR devices, you should use the **show platform hardware qfp active datapath utilization | inc Processing** command for CPU utilization and **show platform hardware qfp active infrastructure exmem statistics | sec DRAM** command for memory utilization.

---

## 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.
-

## LIMITED ORDERABILITY RELEASE

# Change the Polling Interval 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 Policies > My Policies**.
- Step 2** Check 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 multiple 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.
- 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 EPN 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 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** 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 example, which specifies thresholds and alarms for CPU utilization on Cisco ASR 9000 devices.

**LIMITED ORDERABILITY RELEASE**

Policy Types / **Device Health**

\* Device Selection

\* Name  Author

Description  Contact

Feature Category

---

**Parameters and Thresholds**

Show

Parameter	Polling Fr...	Condition	Reaction
▼ CPU Utilization 5 min			
Greater Than 90 Percent(%) 3 times ▼		ALARM MINOR ▼	- +
Greater Than 90 Percent(%) 6 times ▼		ALARM MAJOR ▼	- +
Greater Than 90 Percent(%) 9 times ▼		ALARM CRITICAL ▼	- +
Greater Than ▼	90	Percent(%)	9 times

- 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 EPN 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 for EVCs](#)
- [Performance Test for Optical Circuits](#)

## Generate Performance Reports

Cisco EPN Manager provides reports that monitor:

- Environmental temperature, CPU and memory utilization
- Interface errors and discards
- For Carrier Ethernet devices—IPSLA Ethernet OAM, IPSLA Y.1731, PWE3, QoS performance and interface performance and utilization
- For Optical devices—Ethernet, OTN, physical, and SDH/SONET performance

## ***LIMITED ORDERABILITY RELEASE***

When you run a performance report, retrieves historical data that has been saved in the database. Reports can only display data that Cisco EPN Manager has been configured to collect—in other words, data that is 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 [Reports Available in Cisco EPN Manager](#).