



# Monitor Device and Network Health and Performance

---

- [How Device Health and Performance Is Monitored: Monitoring Policies, on page 1](#)
- [Set Up Basic Device Health Monitoring, on page 2](#)
- [Set Up Basic Interface Monitoring, on page 3](#)
- [Use the Dashboards To Check Network and Device Health, on page 5](#)
- [Check What Cisco EPN Manager Is Monitoring, on page 5](#)
- [Check a Monitoring Policy's Device, Polling, Threshold, and Alarm Settings, on page 8](#)
- [Adjust What Is Being Monitored, on page 8](#)
- [Check the Status of Past Monitoring Policy Data Collections, on page 11](#)
- [Change the Device Set a Policy is Monitoring, on page 11](#)
- [Change the Polling for a Monitoring Policy, on page 12](#)
- [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 12](#)
- [Run Performance Tests, on page 13](#)
- [Monitor Network Performance Using Reports, on page 20](#)

## 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 Cisco EPN 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 EPN 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](#).

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 EPN 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](#).
2. Adjust your policy's polling frequencies or disable polling altogether for specific parameters.
3. Specify the threshold crossing alarms (TCAs) you want Cisco EPN 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 outside 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
<b>Automonitoring</b>	Lists the policies that are enabled by default in Cisco EPN Manager. Only the Device Health monitoring policy is enabled by default. You can adjust the settings for this policy.
<b>My Policies</b>	The policy you create is listed here. When you choose a policy from <b>My Policies</b> , 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 8](#).

## Set Up Basic Interface Monitoring

Interfaces are not monitored by default. This protects the system performance for networks with a large numbers of interfaces.

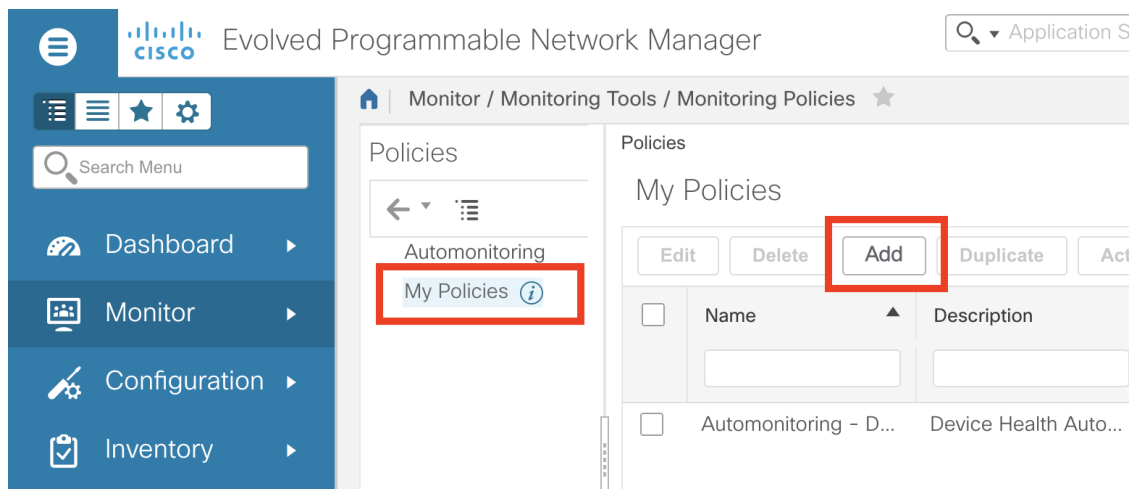
Use this procedure to set up basic interface monitoring.

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 1: 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](#)).

When you select a policy, Cisco EPN 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 EPN 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 EPN 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.

Policies / My Policies

## ASR9K-IF-Health

*Device Selection ▼	
* Name ASR9K-IF-Health	Author root
Description <input type="text"/>	Contact <input type="text"/>
Feature Category Interface Health	Status Active

### Parameters and Thresholds

Parameter	Polling Frequency
▶ Statistics	15 min ▼
▶ CRC	No Polling ▼

**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 12](#).

**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 EPN 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](#).

## Check What Cisco EPN 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 EPN 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 EPN 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 the instructions that follow this table.
Description	Policy description (specified by the policy creator).
Type	Template (policy type) used to create this policy. For information on the policy types, see <a href="#">How Device Health and Performance Is Monitored: Monitoring Policies, on page 1</a> .
Status	<b>Active</b> or <b>Inactive</b> .
Threshold	Whether the policy monitors parameter thresholds and generates TCAs. If <b>Yes</b> is displayed, you can check the TCA settings using the instructions that follow this table.

Policy Field	Description
Activation History	<p>Active monitoring policy—Displays the number of times the policy was activated, and provides a hyperlink to an Activation History popup window that tells you:</p> <ul style="list-style-type: none"> <li>• When the policy was activated.</li> <li>• Which devices were polled at each policy run. If the list is very long, hover your mouse cursor over the list in the <b>Activated for</b> column to launch a popup window.</li> </ul> <p>Inactive monitoring policy—Displays <b>Not Available</b>.</p>
Collection Status	<p>Active monitoring policy—Provides a hyperlink to a Collection Status popup window that tells you:</p> <ul style="list-style-type: none"> <li>• The Device name, IP address, and availability state of each device that was polled by the policy.</li> <li>• Which parameters were polled at each policy run. If the list is very long, hover your mouse cursor over the list in the <b>Parameters</b> column to launch a popup window.</li> </ul> <p>Inactive monitoring policy—Displays <b>Not Available</b>.</p>

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](#).

Policy Field	Description
General Information	Name, description, creator, status, policy type (Feature Category). For information on the policy types, see <a href="#">How Device Health and Performance Is Monitored: Monitoring Policies, on page 1</a> .
Device Selection	Devices which the policy is monitoring.
Polling Frequency	How often Cisco EPN Manager polls the device parameters.

Policy Field	Description
Parameters and Thresholds	Which parameters are polled and their TCA settings, if any. To view the TCA settings, click the arrow next to the parameter name. For more information about viewing the parameters polled by the various policy types, see <a href="#">Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 7</a> .

## Check Which Parameters and Counters Are Polled By a Monitoring Policy

[Check What Cisco EPN Manager Is Monitoring, on page 5](#) 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](#).

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:**

- Click **Edit**. The supported policy types are listed in the navigation area on the left.
- 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 11](#).
- 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 12](#).
- 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 12](#).
- Optical policy thresholds cannot be customized.
- 

## Adjust What Is Being Monitored

To make adjustments to what Cisco EPN Manager is monitoring, use the guidance in the following table to find the best method for your needs.



If:		See:
Cisco EPN Manager is collecting the data you need, and...	... you want to change the polling frequency	<a href="#">Change the Polling for a Monitoring Policy, on page 12</a>
	... you want to adjust the alarm behavior	<a href="#">Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 12</a>
	... you want to adjust which devices are monitored	<a href="#">Change the Device Set a Policy is Monitoring, on page 11</a>
Cisco EPN Manager is <i>not</i> collecting the data you need, and...	... a similar monitoring policy already exists	<a href="#">Create a New Monitoring Policy Based On An Existing Policy, on page 9</a>
	... no similar monitoring policies exist, but one of the policy types contains the parameters you want to monitor	<a href="#">Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 10</a>
	... no similar monitoring policies exist, and none of the policy types contain the parameters you want to monitor	<a href="#">Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 10</a>
	... 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 EPN Manager Is Monitoring, on page 5](#).
- Step 2** Create the duplicate.
- Choose **Monitor > Monitoring Tools > Monitoring Policies**, then click **My Policies** from the list on the left.
  - Locate the policy you want to duplicate.
  - Select the policy, then click **Duplicate**.
  - 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.
- Locate the policy under **My Policies**.
  - Select the policy and click **Edit**.
  - Make your changes as needed. See:
    - [Change the Device Set a Policy is Monitoring, on page 11](#)
    - [Change the Polling for a Monitoring Policy, on page 12](#)
    - [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 12](#)
- 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 New Monitoring Policy Using Out-of-the-Box Policy Types

---

- Step 1** Check what is currently being monitored. See [Check What Cisco EPN Manager Is Monitoring, on page 5](#).
- 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:
- 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 for a Monitoring Policy, on page 12](#) and [Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 12](#).
- 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.

**Step 7** To view the MIB polling data, create a generic dashlet on the Performance dashboard using the name of the policy that you created.

**Note** The option to create a generic dashlet is available only on the **Device Trends** page.

**Note** To view the SNMP polling date 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.

---

## 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 EPN 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.

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

**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 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 Based on Y.1564 for EVCs](#)
- [Performance Test Based on Y1731 for EVCs](#)
- [Performance Test for Optical Circuits](#)
- [Performance Test for Circuit Emulation Services](#)

Cisco EPN 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 14](#).

## 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 16.
- 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

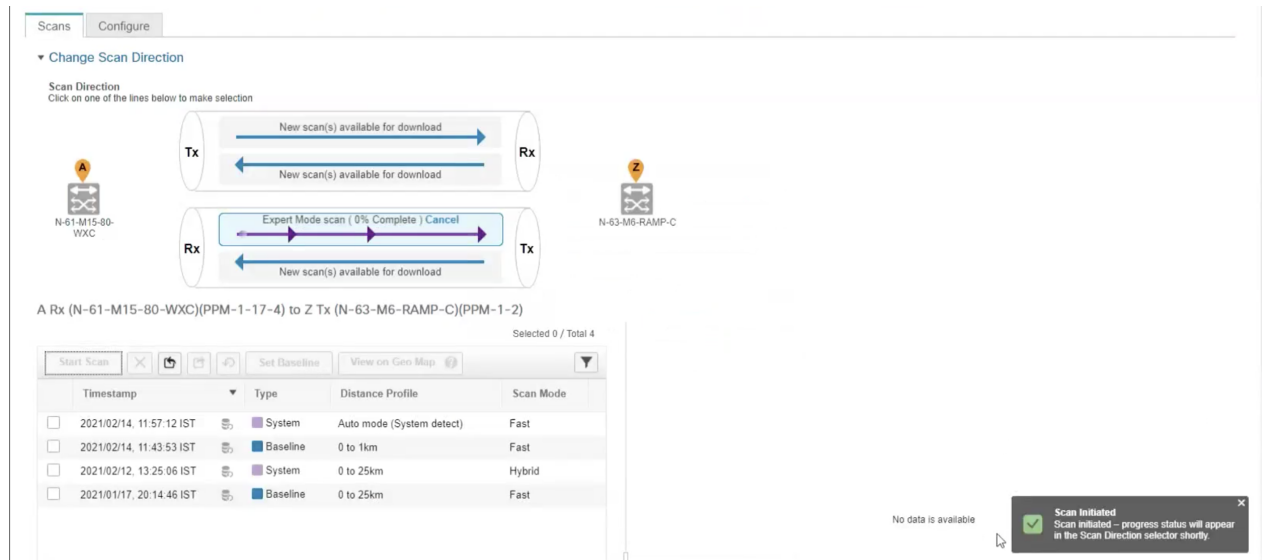
Once the scan is complete,

- 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 19](#)

Figure 2: 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 18](#).

**Step 9** To import the scans, see [Import OTDR Scan, on page 18](#).

**Step 10** To schedule the OTDR scan to be run at predefined regular intervals, see [Provision OTDR Scan Recurrence, on page 18](#).

## 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* 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](#).

**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 18](#).
- 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 18](#).
- Intervals—To schedule a granular recurring scan, go to [Step 5, on page 18](#).

**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

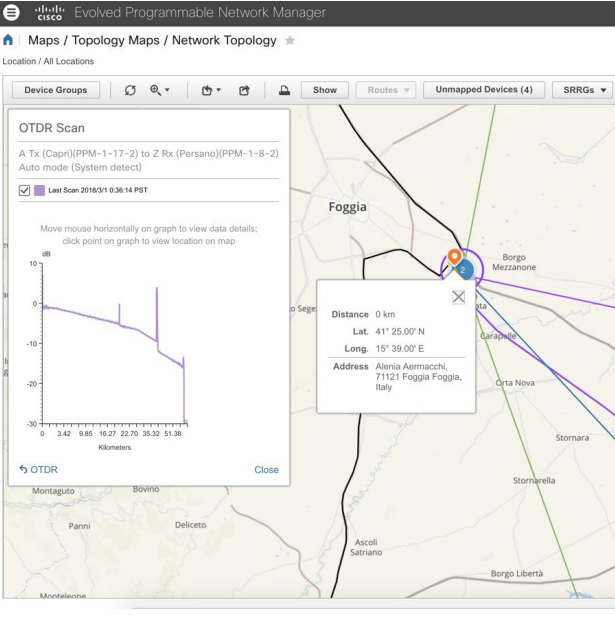
You can view the OTDR scan results in the context of the geo map in order to pinpoint the location of the fiber issues. For example, if the OTDR test reports a concentrated loss 20 km from the link endpoint, you can visualize on the map where this is geographically located.

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](#).
- The OTS link on which the OTDR scan is run must be associated with a fiber. See [Associate Links to Fibers](#).
- The A- and Z-side devices must be mapped on the geo map. See [Place Unmapped Devices on the Geo Map](#).

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	Launch the OTDR scan.	
<b>Step 2</b>	Define the scan parameters and run the scan.	
<b>Step 3</b>	Click <b>View on Geo Map</b> .	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).
<b>Step 4</b>	Click on a point in the OTDR scan results graph.	<p>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.</p> <p><b>Note</b> 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.</p>

	Command or Action	Purpose
		 <p>The screenshot shows the Cisco Evolved Programmable Network Manager interface. The main view is a map titled 'Maps / Topology Maps / Network Topology'. An 'OTDR Scan' window is open, displaying a line graph of scan results. The graph shows a signal loss over distance, with a peak at approximately 35.32 kilometers. A tooltip is visible over the map, showing coordinates and an address: 'Alenia Aermacchi, 71121 Foggia Foggia, Italy'.</p>
<p><b>Step 5</b></p>	<p>If necessary, click on the <b>OTDR</b> link below the OTDR scan results graph to return to the OTDR scan page.</p>	

## Monitor Network Performance Using Reports

Cisco EPN 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 EPN 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](#).



**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`