Monitor Device and Network Health and Performance

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 will be displayed in dashboards, reports, the Alarms and Events table, and other areas of the web GUI.

To view and administer monitoring policies, choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**.

Navigation	Description
Automonitoring	Lists the policies that are enabled by default in Cisco EPN Manager . Only the Device Health monitoring policy is enabled by default. You can adjust the settings for this policy.
My Policies	The policy you create is listed here. When you choose a policy from **My Policies**, you can view the policy's details.

Set Up Basic Device Health Monitoring

The Device Health monitoring policy is enabled by default. It 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 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 9.

Set Up Basic Interface Monitoring

Interfaces are not monitored by default. This protects system performance for networks with 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** from the list on the left.

Step 2   Click **Add** to create a new policy.
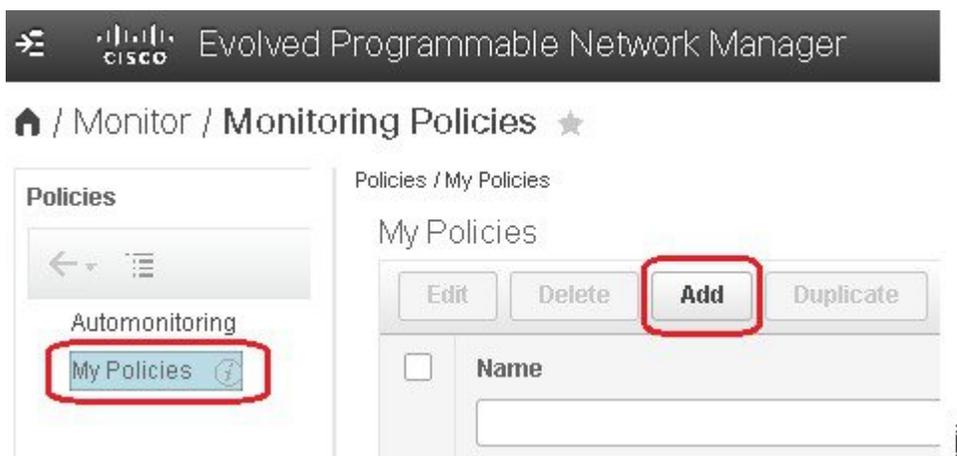
Step 3   Choose **Interface Health** for generic interface monitoring. If you are monitoring optical devices, choose **Optical 15 Mins** or another optical policy (see Monitoring Policies Reference).
When you select a policy, Cisco EPN Manager populates the window with the policy settings.

Step 4   Enter a meaningful name and description.

Step 5   From the **Device Selection** drop-down list, select the devices (or device groups) you want to monitor. 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 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 parameters.
For example, the following shows a policy that will monitor Cisco ASR 9000 interfaces. It uses the **Interface Health** policy type, where a all parameters are polled using the same interval.

Policy Types

Interface Health

* Device Selection

* **Name**   ASR9K-IF-Health

Description

Feature Category Interface Health

Parameters and Thresholds

Polling Frequency   15 min

15 min

1 min

5 min

1 hour

Parameter

- ▶ Inbound Disca
- ▶ Outbound Discards Percentage
- ▶ Inbound Errors Percentage
- ▶ Outbound Errors Percentage
- ▶ Input Utilization Percentage
- ▶ Output Utilization Percentage

Save and Activate ▾   Cancel

410591

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.

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 13.

Step 8   Click:

   • **Save and Activate** to start monitoring immediately

   • **Save and Close** to save the policy and activate it at a later time

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 reachability 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 How Device Health and Performance Is Monitored: Monitoring Policies, on page 1.
Status	**Active** or **Inactive**.
Threshold	Whether the policy monitors parameter thresholds and generates TCAs. If **Yes** is displayed, you can check the TCA settings using the instructions that follow this table.
Activation History	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: • When the policy was activated. • Which devices were polled at each policy run. If the list is very long, hover your mouse cursor over the list in the **Activated for** column to launch a popup window. Inactive monitoring policy—Displays **Not Available**.

Policy Field	Description
Collection Status	Active monitoring policy—Provides a hyperlink to a Collection Status popup window that tells you: • The Device name, IP address, and reachability state of each device that was polled by the policy. • Which parameters were polled at each policy run. If the list is very long, hover your mouse cursor over the list in the **Parameters** column to launch a popup window. Inactive monitoring policy—Displays **Not Available**.

To view polling frequencies and TCA details, from **My Policies**, select a policy from the list on the left. Depending on the policy type, the following information is displayed.

Note   The Optical 1 day and Optical 15 minutes policies do not display polled parameters in the web GUI. That information is provided in Monitoring Policies Reference.

Policy Field	Description
General Information	Name, description, creator, status, policy type (Feature Category). For information on the policy types, see How Device Health and Performance Is Monitored: Monitoring Policies, on page 1.
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 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 Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 7.

Check Which Parameters and Counters Are Polled By a Monitoring Policy

Check What Cisco EPN Manager Is Monitoring, on page 6 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   Because Optical 1 Day and Optical 15 Mins parameters are not displayed in the web GUI, they are listed in 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 useful if you want to check what a new policy will poll before creating the policy.

Step 1 Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then choose **My Policies**. The web GUI lists the existing active and inactive monitoring policies.

Step 2 **To check the parameters used by an existing policy**:

• To view parameters that were polled most recently, locate the policy in the window on the right, then click **Details** in the **Collection Status** column. In the Collection Data dialog box, hover your mouse over the text in the **Parameter** column to list the polled parameters.

• To view the parameters along with their polling settings, expand **My Policies** in the navigation area on the left, then choose the policy you want to check. The window on the right displays the parameters and their polling settings.

Step 3 **To check the parameters used by a specific policy type**:

a) Click **Edit**. The supported policy types are listed in the navigation area on the left.
b) Choose a policy type. The window on the right displays the parameters polled by that policy, along with default polling and TCA settings. (These settings can be customized when a monitoring policy is created.)

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 12.

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 13.
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	Change the Polling for a Monitoring Policy, on page 12
	... you want to adjust the alarm behavior	Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 13
	... you want to adjust which devices are monitored	Change the Device Set a Policy is Monitoring, on page 12
Cisco EPN Manager is *not* collecting the data you need, and...	... a similar monitoring policy already exists	Create a New Monitoring Policy Based On An Existing Policy, on page 9
	... no similar monitoring policies exist, but one of the policy types contains the parameters you want to monitor	Create a New Monitoring Policy Using Out-of-the-Box Policy Types, on page 10
	... no similar monitoring policies exist, and none of the policy types contain the parameters you want to monitor	Create a Monitoring Policy for Unsupported Parameters and Third-Party Devices, on page 10
	... 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 6.

Step 2 Create the duplicate.

a) Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, then click **My Policies** from the list on the left.

b) Locate the policy you want to duplicate.

c) Select the policy, then click **Duplicate**.

d) In the **Duplicate Policy Creation** dialog, choose the parent folder, enter a policy name and description, then click **OK**.

Step 3 Make your changes to the duplicate.

a) Locate the policy under **My Policies**.

b) Select the policy and click **Edit**.

c) Make your changes as needed. See:

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 6.

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. To check which policies can be applied to port groups, see Check What Cisco EPN Manager Is Monitoring, on page 6.

Step 4   Configure the new policy:

    a) Select the devices, device groups, or port groups from the **Device Selection** drop-down list. (Not all monitoring types can be applied to port groups.)

    b) Enter a name and contact, and edit the description.

    c) Under **Parameters and Thresholds**, configure the polling settings, parameter values, and alarm conditions. See Change the Polling for a Monitoring Policy, on page 12 and Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 13.

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 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 on the Performance dashboard using the name of the policy that you created.

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 an severity) when a problem is detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds or alarms associated with it.

Step 1   Choose **Monitor** > **Monitoring Tools** > **Monitoring Policies**, 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.

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 performance tests on OTS optical links. For more information, see Run a Performance Test on a Link (OTS Link).

Monitor Network Performance Using Reports

Cisco EPN Manager provides a variety of 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 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.