Monitor Device and Network Health and Performance

This chapter contains the following topics:

How Device Health and Performance Is Monitored: Monitoring Policies

Monitoring policies control how monitors your network by controlling the following:

- What is monitored—The network and device attributes 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 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 . 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.

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 and make it easy for you to start monitoring different technologies and services.
2. Adjust your policy's polling frequencies or disable polling altogether for specific parameters.
3. Specify the threshold crossing alarms (TCAs) you want 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 . Only the Device Health monitoring policy is enabled by default. You can adjust the settings for this policy.
My Policies	The policy you create is listed here. When you choose a policy from My Policies, you can view the policy's details.

Set Up Basic Device Health Monitoring

The Device Health monitoring policy is enabled by default. It monitors both Cisco devices and third-party devices. For Cisco devices, the device health monitoring checks managed devices for CPU utilization, memory pool utilization, environment temperature, and device availability. For third party devices, the device health monitoring checks managed devices for device availability only. This policy also specifies thresholds for utilization and temperature which, if surpassed, trigger alarms that are displayed in the GUI client.

To view the current settings for this policy, choose Monitor > Monitoring Tools > Monitoring Policies, then select Automonitoring from the list on the left. You can also adjust the polling frequency and threshold for the different parameters. To adjust a polling frequency or threshold, use the drop-down lists that are provided in the GUI client.

You might also want to create a device health monitoring policy that monitors specific devices—for example, devices of a certain type or in a certain geographical location. For instructions on how to do this, see Adjust What Is Being Monitored, on page 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.

When you select a policy, populates the window with the policy settings.

Step 4 Enter a meaningful name and description.

Step 5 From the Device Selection drop-down list, click the appropriate radio button and then select the devices or device groups you want to monitor. If you chose the Interface Health monitoring policy, you can also select port groups.

only lists the devices or ports applicable to the policy 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 , the Interface Health monitoring policy polls all of 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 parameters.

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 16.

Step 8 Click:

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

Default Monitoring Policies

Prime Infrastructure polls SNMP objects to gather monitoring information for the following health monitoring policies under Monitor > Monitoring Tools > Monitoring Policies > Automonitoring:

- Device Parameters—The table Device Parameter Automonitoring Metrics describes the device health parameters that are polled.
- Interface Parameters—The table Interface Parameter Automonitoring Metrics describes the interface parameters that are polled for:
  - Trunk and Link Ports
  - WAN Interfaces

For the following monitoring policies that provide assurance information, data is collected through NetFlow or NAMs:

- Application Response Time

- NAM Health
- Traffic Analysis
- Voice Video Data
- Voice Video Signaling

Table 1: Device Parameter Automonitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
Device Availability	All SNMP devices, Third Party devices	SNMPv2-MIB	sysUpTime
CPU Utilization	Cisco IOS devices, All Supported Nexus devices, Cisco UCS devices	CISCO-PROCESS-MIB	cpmCPUTotalPhysicalIndex cpmCPUTotal1minRev
	Cisco ASR device	CISCO-ENTITY-QFP-MIB	
Memory Pool Utilization	Cisco IOS devices, ISR devices.	CISCO-MEMORY-POOL-MIB	ciscoMemoryPoolName ciscoMemoryPoolType ciscoMemoryPoolUsed ciscoMemoryPoolFree
	All supported Cisco Nexus devices, Cisco UCS devices and Cisco IOS XE devices	CISCO-PROCESS-MIB	cpmCPUTotalIndexcpmCPUMemoryUsedcpmCPUMemoryFree
	Cisco ASA devices, IOS XR and Edison devices	CISCO-ENHANCED-MEMPOOL-MIB	cempMemPoolTypecempMemPoolNamecempMemPoolUsedcempMemPoolFree
	Cisco IOS ASR devices	CISCO-ENTITY-QFP-MIB	ceqfpMemoryResTypeceqfpMemoryResInUseceqfpMemoryResFree
Environment Temp[1]	ASR, All Supported Nexus devices, Cisco UCS devices	CISCO-ENVMON-MIB	entSensorValue
	Catalyst 2000, 3000, 4000, 6000, ISR	CISCO-ENVMON-MIB	ciscoEnvMonTemperatureStatusValue

[1] For stacked switch devices, the Environment Temp displays the temperature of each stacked instance.

Table 2: Interface Parameter Automonitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
Interface Availability	Cisco IOS devices, All Supported Nexus devices, and Third Party devices	IF-MIB	ifOperStatus

Metric	Devices Polled	MIB	MIB Objects Included
Input Utilization	Cisco IOS devices, Third Party devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCInBroadcastPkts, ifHCInMulticastPkts, ifInErrors, ifInDiscards, ifInUnknownProtos ifHCInBroadcastPkts, ifHCInMulticastPkts, locIfInputQueueDrops
Output Utilization	Cisco IOS devices, Third Party devices	IF-MIB, Old-CISCO-Interface-MIB	ifHCOutBroadcastPkts, ifHCOutMulticastPkts, ifHCOutUcastPkts, ifOutDiscards, ifOutUnknownProtos, locIfOutputQueueDrops
Percent Drop per QoS Class	Cisco IOS devices	IF-MIB, Old-CISCO-Interface-MIB	cbQosCMDropBitRate,cbQosCMPrePolicyBitRate

Note locIfIn, outQueueDrops, and QOS monitoring are not supported for third party devices.

Table 3: Class-Based, QoS, Health-Monitoring Metrics

Metric	Devices Polled	MIB	MIB Objects Included
QOS calculation	Cisco IOS devices	CISCO-CLASS-BASED-QOS-MIB	cbQosCMDropByte64 cbQosCMPostPolicyByte64 cbQosCMPrePolicyByte64
Interface Inbound Errors	Cisco IOS devices, Third party devices	IF-MIB	ifInErrors
Interface Outbound Errors	Cisco IOS devices, Third party devices	IF-MIB	ifOutErrors
Interface Inbound Discards	Cisco IOS devices, Third party devices	IF-MIB	ifInDiscards
Interface Outbound Discards	Cisco IOS devices, Third party devices	IF-MIB	ifOutDiscards

Modify Default Monitoring Policies

Prime Infrastructure monitoring policies monitor network device metrics and alert you of changing conditions before the issues impact their operation. By default, Prime Infrastructure polls device health metrics on supported routers, switches and hubs and third party devices, and interface health metrics on WAN interfaces, links, and trunk ports. It is not polled on storage devices, and UCS series devices. If a the threshold is violated three times, Prime Infrastructure generates a critical alarm, which is displayed on the Monitor > Monitoring Tools > Alarms and Events page.

To modify or disable the polling frequency and the threshold parameters, follow these steps:

Step 1 Choose Monitor > Monitoring Tools > Monitoring Policies > Automonitoring.

Step 2 Select Device Health, then modify the polling frequencies and thresholds as desired.

Step 3 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.

Use the Dashboards To Check Network and Device Health

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.

For information on dashboards, see Set Up and Use the Dashboards.

Check What Is Monitoring

This topic explains how to get the following information:

- Which policies are activated, their status, and their history.
- The specific parameters that 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. 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.
	Policy description (specified by the policy creator).

Policy Field	Description
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.
Collection Status	Active monitoring policy—Provides a hyperlink to a Collection Status popup window that tells you: • 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.

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 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 Check Which Parameters and Counters Are Polled By a Monitoring Policy, on page 8.

Check Which Parameters and Counters Are Polled By a Monitoring Policy

Check What 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.

You can use this procedure to check:

- Parameters polled by existing policies (regardless of whether a policy is active or inactive).
- Parameters used by a policy type. This is useful if you want to check what a new policy will poll before creating the policy.

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

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

- To view parameters that were polled most recently, locate the policy in the window on the right, then click Details in the Collection Status column. In the Collection Data dialog box, hover your mouse over the text in the Parameter column to list the polled parameters.
- To view the parameters along with their polling settings, expand My Policies in the navigation area on the left, then choose the policy you want to check. The window on the right displays the parameters and their polling settings.

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

a) Click Edit. The supported policy types are listed in the navigation area on the left.

b) Choose a policy type. The window on the right displays the parameters polled by that policy, along with default polling and TCA settings. (These settings can be customized when a monitoring policy is created.)

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 15.

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 16.

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 16.

Adjust What Is Being Monitored

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

If:		See:
is collecting the data you need, and...	... you want to change the polling frequency	Change the Polling for a Monitoring Policy, on page 16
	... you want to adjust the alarm behavior	Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 16
	... you want to adjust which devices are monitored	Change the Device Set a Policy is Monitoring, on page 15
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 14
	... 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 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:

- Change the Device Set a Policy is Monitoring, on page 15
- Change the Polling for a Monitoring Policy, on page 16
- Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 16

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 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.

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 16 and Change Thresholds and Alarm Behavior for a Monitoring Policy, on page 16.

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.

GETVPN Monitoring Policies

For the GETVPN policy type, Prime Infrastructure uses metrics described in the following table.

Table 4:

GETVPN Monitoring Parameters	MIB	MIB Objects Included
Group Name Group ID Group ID Type Group ID Length Key Server ID Group Member ID Device Type Device ID Device ID Type Device ID length Registered Key Server ID Registered Key Server ID Type Registered Key Server ID Length	CISCO-GDOI-MIB	gmGdoiGroupTable cgmGdoiGroupName, cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGroupIdLength cgmGdoiKeyServerTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiKeyServerIdValue, cgmGdoiKeyServerIdType, cgmGdoiKeyServerIdLength, cgmGdoiKeyServerActiveKEK, cgmGdoiKeyServerRekeysPushed cgmGdoiKsKekTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiKeyServerIdValue, cgmGdoiKeyServerIdType, cgmGdoiKsKekIndex, cgmGdoiKsKekSPI, cgmGdoiKsKekSrcIdValue, cgmGdoiKsKekSrcIdType, cgmGdoiKsKekSrcIdLength, cgmGdoiKsKekDstIdValue, cgmGdoiKsKekDstIdType, cgmGdoiKsKekDstIdLength, cgmGdoiKsKekOriginalLifetime, cgmGdoiKsKekRemainingLifetime

GETVPN Monitoring Parameters	MIB	MIB Objects Included
Active KEK Rekeys Count KEK Index KEK SPI KEK Source ID KEK Source ID Type KEK Source ID Length KEK Destination ID KEK Destination ID Type KEK Destination ID Length KEK Original Lifetime KEK Remaining LIfetime TEK Selector Index TEK Source ID TEK Source ID Type TEK Source ID Length TEK Destination ID TEK Destination ID Type TEK Destination ID Length TEK Policy Index TEK SPI TEK Original Lifetime TEK Remaining Lifetime TEK Window Size	CISCO-GDOI-MIB	cgmGdoiKsTekSelectorTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiKeyServerIdValue, cgmGdoiKeyServerIdType, cgmGdoiKsTekSelectorIndex, cgmGdoiKsTekSrcIdValue, cgmGdoiKsTekSrcIdType, cgmGdoiKsTekSrcIdLength, cgmGdoiKsTekDstIdValue, cgmGdoiKsTekDstIdType, cgmGdoiKsTekDstIdLength cgmGdoiKsTekPolicyTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiKeyServerIdValue, cgmGdoiKeyServerIdType, cgmGdoiKsTekPolicyIndex, cgmGdoiKsTekSPI, cgmGdoiKsTekOriginalLifetime, cgmGdoiKsTekRemainingLifetime, cgmGdoiKsTekWindowSize cgmGdoiGmTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmIdLength, cgmGdoiGmRegKeyServerIdValue, cgmGdoiGmRegKeyServerIdType, cgmGdoiGmRegKeyServerIdLength, cgmGdoiGmActiveKEK, cgmGdoiGmRekeysReceived cgmGdoiGmKekTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmKekIndex, cgmGdoiGmKekSPI, cgmGdoiGmKekSrcIdValue, cgmGdoiGmKekSrcIdType, cgmGdoiGmKekSrcIdLength, cgmGdoiGmKekDstIdValue, cgmGdoiGmKekDstIdType, cgmGdoiGmKekDstIdLength, cgmGdoiGmKekOriginalLifetime, cgmGdoiGmKekRemainingLifetime cgmGdoiGmTekSelectorTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmTekSelectorIndex, cgmGdoiGmTekSrcIdValue, cgmGdoiGmTekSrcIdType, cgmGdoiGmTekSrcIdLength, cgmGdoiGmTekDstIdValue, cgmGdoiGmTekDstIdType, cgmGdoiGmTekDstIdLength cgmGdoiGmTekPolicyTable cgmGdoiGroupIdValue, cgmGdoiGroupIdType, cgmGdoiGmIdValue, cgmGdoiGmIdType, cgmGdoiGmTekPolicyIndex, cgmGdoiGmTekSPI, cgmGdoiGmTekOriginalLifetime, cgmGdoiGmTekRemainingLifetime, cgmGdoiGmTekWindowSize

DMVPN Monitoring Policies

For the DMVPN policy type, Prime Infrastructure uses metrics described in the following table.

Table 5: Monitor > Monitoring Tools > Monitoring Policies > DMVPN Metrics

DMVPN Monitoring Parameters	MIB	MIB Objects Included
Remote Peer Physical IP Decrypted Byte Count Encrypted Byte Count Remote Tunnel IP NHRP Expiration Remote Subnet IP Remote Subnet Mask	CISCO-IPSEC-FLOW-MONITOR-MIB	cipSecTunnelTable cipSecTunRemoteAddr, cipSecTunInOctets, cipSecTunOutOctets
	NHRP-MIB	nhrpCacheTable nhrpCacheInternetworkAddr, nhrpCacheHoldingTime, nhrpCacheNbmaAddr, nhrpCacheType
	IP-FORWARD-MIB	pCidrRouteTable ipCidrRouteNextHop, ipCidrRouteDest, ipCidrRouteMask

LISP Monitoring Policy

For the LISP monitoring policy type, <Product Name> uses the metrics shown in the following table.

Table 6: Monitor > Monitoring Tools > Monitoring Policies > LISP Monitoring

LISP Monitoring Parameters	MIB	MIB Objects Included
LISP Map Cache Size	LISP-MIB	lispFeaturesMapCacheSize
LISP Map Cache Limit	LISP-MIB	lispFeaturesMapCacheLimit

You can view the polled data in the Device Lisp Map Cache Entries dashlet under Device dashboard and in the Top N Lisp Map Cache Entries dashlet under the Network Devices dashboard.

Nexus Virtual Port Channel (VPC) Health Monitoring Policy

The Nexus VPC health monitoring policy periodically fetches the configuration parameters from the primary VPC configured Nexus Switch and looks for any discrepancies in the configuration that can lead to inconsistencies, by correlating with the secondary VPC configured Nexus Switch. If inconsistencies are detected the monitoring policy generates an alarm and captures the details of the inconsistency at global level and VPC level. The following table describes the Nexus VPC Health Monitoring policy parameters.

Table 7: Monitor > Monitoring Tools > Monitoring Policies > Nexus VPC Health

Category	Nexus VPC Monitoring Parameters
Global Fault	stpModestp, Disabled, stpMstRegionName, stpMstRegionRevision, stpMstRegionVlanMap, stpLoopguard, stpBridgeAssurance, stpEdgePortType, bpduFilterGuard, stpMstSimulatePvst, passVlans
VPC Fault	VpcCardType, OperationalPortMode, Mode, LacpMode, InterfaceType, AdminPortMode, Speed, Duplex, Mtu, NativeVlan,StpPortType, StpPortGuard, StpMstSimulatePvst

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 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 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.

Example: Monitor IP SLA

You can create a monitoring policy to view IP service levels for network-based applications and services. There are approximately seven IP SLA-related MIBs. In this example, the video MIB only is monitored.

Step 1 Download the IP SLA video MIB from the following URL: http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2

Step 2 ChooseMonitor > Monitoring Policies > My Policies, then click Add.

Step 3 Click Custom MIB Polling.

Step 4 Enter a name for the policy.

Step 5 Under the MIB Selection tab, click Upload MIB and navigate to the MIB that you uploaded in Step 1.

Step 6 From the Tables pulldown menu, select a table, then select the specific metrics to monitor.

Step 7 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 8 Select the devices for which you want to monitor IP SLA metrics.

Step 9 Click Save and Activate to immediately activate the policy on the devices specified.

Step 10 To monitor this information from a dashboard, you need to create a generic dashlet. See Add a Predefined Dashlet To a Dashboard for more information.

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.

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

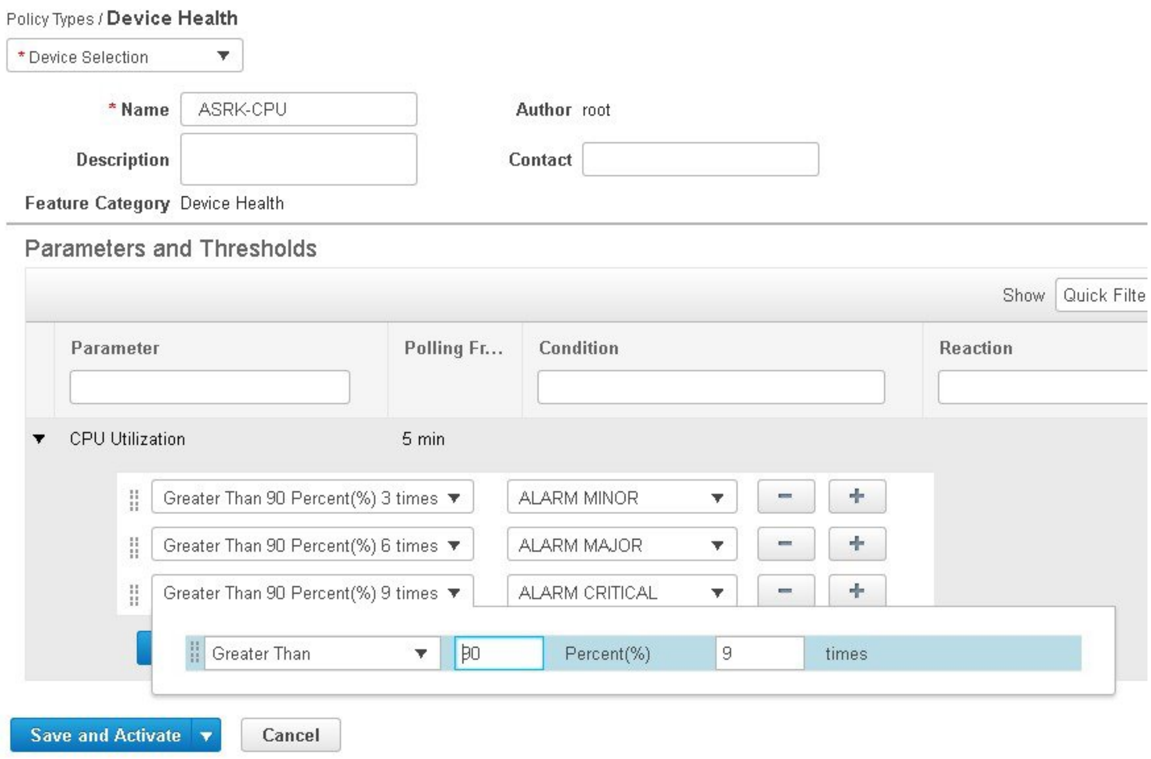
You can customize the threshold value that indicates a problem and whether should generate an informational event or an alarm (of any severity) when a problem is detected. Not all policies have all of these settings; for example, a policy may only collect statistics, so it would not have any thresholds 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.

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: ASRK-CPU

Author: root

Description:

Contact:

Feature Category: Device Health

Parameters and Thresholds

Show: Quick Filte

Parameter	Polling Fr...	Condition	Reaction
CPU Utilization	5 min		

Condition	Reaction
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.

Metrics	Parameters
CPU	CPU Utilization
MEMORY	Memory Pool Utilization
ENVTEMP	Environment Temperature
INTERFACE	Interface Inbound Errors, Interface Outbound Errors, Interface Inbound Discards, Interface Outbound Discards, Input Utilization, Output Utilization, Input Packet Broadcast Percent, Percentage drops in input queue, Percentage drops in output queue
QOS	Percent Drop per QoS Class

Policy Name	Parameters
Traffic Analysis	In Bytes, In Packets, Out Bytes, Out Packets
Traffic Analysis	Total Bytes, Total Packets, In Bytes, In Packets, Out Bytes, Out Packets

Policy Name	Parameters
Application Response Time	Average Network Time, Average Client Network Time, Average Server Network Time, Average Transaction Time, Average Server Response Time, Maximal Network Time, Maximal Client Network Time, Maximal Server Network Time, Maximal Transaction Time
Voice Video Data	Average MOS, Worst MOS, Jitter, Actual Packet Loss, Adjusted Packet Loss

Monitor Network Performance Using Reports

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

When you run a performance report, retrieves historical data that has been saved in the database. Reports can only display data that 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.) .