



Monitor Network Health and KPIs

This section contains the following topics:

- [Health Insights Overview, on page 1](#)
- [Manage KPIs, on page 7](#)
- [Manage KPI Profiles, on page 17](#)
- [Troubleshoot Health Insights, on page 24](#)

Health Insights Overview

Health Insights is a network health application that performs real-time key performance indicator (KPI) monitoring, analytics, alerting, and troubleshooting. Health Insights builds dynamic detection and analytics modules that allow operators to monitor and alert network events with user-defined logic.

Health Insights provides prebuilt KPIs that are based on model-driven and SNMP-based telemetry. The Health Insights Recommendation Engine uses data mining to analyze your network and then recommends which telemetry paths you should enable and monitor.



Note For the recommendation engine to work in Health Insights, you need to ensure that direct connectivity is established between Cisco Crosswork Change Automation and Health Insights and the device, and enable the NETCONF protocol.

The following high-level example shows how Health Insights interacts with the other Cisco Crosswork Network Automation components:

1. Health Insights detects an anomaly: The optical bit error rate that you are monitoring on each of the links in your network suddenly increases.
2. Change Automation Playbooks automate remediation: Switch to the backup link immediately. Restore service. Open a ticket (manually initiated by the user). Alert the network engineer.

Any network remediation can be orchestrated via Change Automation Playbooks, which closes the loop on problem detection and resolution.

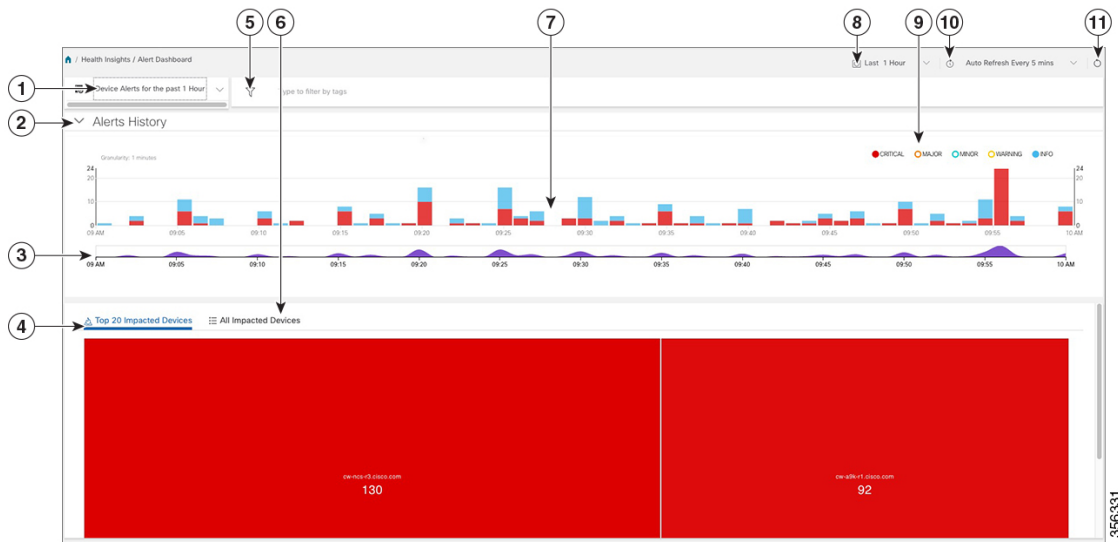
Health Insights Alert Dashboard

The Health Insights alert dashboard provides device health summary information that is based on real-time network state events. The dashboard displays a network view of KPI sensors that are paired to specific device groups. Health Insights raises customizable events and alerts that are based on user-defined logic.



Note Alert dashboard displays individual KPI alerts, even though the mechanism of enabling KPI on a device is done through a KPI profile.

To display the Health Insights dashboard, choose **Performance Alerts > Alert Dashboard** from the main menu.



Item	Description
1	Device/KPI Alert Selector: Click here to toggle between device alert and KPI alert information.
2	Alerts History: This dashlet shows the total number of device alerts or KPI alerts that have been raised during the chosen time period, with detailed time lines showing both individual sets of alerts and the overall alert trend.

Item	Description
3	<p>Alerts Trend Line: This line shows the overall trend in alerts for the chosen time period. You can use the Alerts Trend Line to select and zoom in on a specific time period within the Alerts History Line, as follows:</p> <ol style="list-style-type: none"> 1. Click the time-period starting point in the Alerts Trend Line and hold down the mouse. 2. Drag the cursor to the endpoint and then release the mouse. <p>The time range you selected is indicated by light gray shading on the Alerts Trend Line, with + and - zoom icons shown above the Alerts History Line. Click the + icon to zoom in on the time range you selected. Click the - to zoom out. To restore the full view of the Alerts History Line, click on any point outside of the light gray shading on the Alerts Trend Line.</p>
4	<p>Top 20 Impacted Devices/ Top 20 Impacted KPIs: When selected, this dashlet displays a map of tiles, each tile representing one of the 20 devices or KPIs with the most alerts during the selected time period. The amount of space that each tile occupies in the map corresponds to the number of alerts raised: the more alerts, the bigger the tile. To view more detailed information for a particular device or KPI, click the device or KPI name link in the center of the tile.</p>
5	<p>Filter By Tags: This field lets you filter the alert dashboard information by associated tag names. To select a tag, do one of the following:</p> <ul style="list-style-type: none"> • If you know the tag that you want to use, enter it in the Type to filter by Tags field and then check its check box. Repeat this step to select more tags. • If you want to select a tag from the tags that are currently available: <ol style="list-style-type: none"> 1. In the Type to filter by Tags field, type any character to open the results list. 2. Click the View All Tags link at the bottom of the list. 3. Check the check box for each tag you want to use and then click Apply Filters. 4. Delete the character that you typed in Step 1 to clear the results list. <p>Tag filters you create are not saved. If you open another window and then return to the alert dashboard, you will need to re-create tag filters.</p>

Item	Description
6	<p>All Impacted Devices/All Impacted KPIs: When selected, this dashlet provides a complete list of all devices or KPIs affected by alerts. The information for each affected device or KPI includes:</p> <ul style="list-style-type: none"> • Device Name or KPI Name • Device or KPI Type • IP address: The IP address of the impacted device. This column is only displayed for devices. • Alert count: The total number of alerts for that device or KPI during the selected period. • Impact score—This value is determined using the following formula: (4 x number of critical alerts) + (3 x number of major alerts) + (2 x number of minor alerts) + number of warning alerts. When monitoring the health of your network, focus on devices or KPIs with a higher impact score. • Severity distribution—Provides a visual breakdown of the severity that is associated with a device or KPI's alerts. To view a tooltip that indicates the number of raised alarms (by severity and in total), place your cursor over the appropriate bar segment.
7	<p>Alerts History: The Alerts History line shows alerts as discrete bar indicators whose height represents the total number of alerts gathered at each point in time. To see the total for each type of alert, hover your mouse cursor over the bar indicator. You can also use the Alerts Trend line to zoom in on particular portions of the alert history.</p>
8	<p>Time Period: Specifies the time period for which the dashboard provides alert information: The past one hour, past day, past week, and so on. Please note that the dashboard provides alert information only, not telemetry information.</p>
9	<p>Severity Legend: Maps the bar indicator colors that are used in the Alert History dashlet to the corresponding alert severity. To display or hide the alerts for a particular severity, click the circle representing that severity. A filled circle indicates that alerts of that severity have been raised and are being displayed. An empty circle indicates that alerts of that severity are either not being displayed or have not been raised during the displayed time period.</p>
10	<p>Auto Refresh: Specifies how often the dashboard is automatically refreshed.</p>
11	<p>Refresh Icon: Refreshes the dashboard.</p>

**Note**

- Alert group logic does not show the alerts impacted on dashboard, only API shows the impacted results.
- Composite Alerting is not displayed in the Alert dashboard.

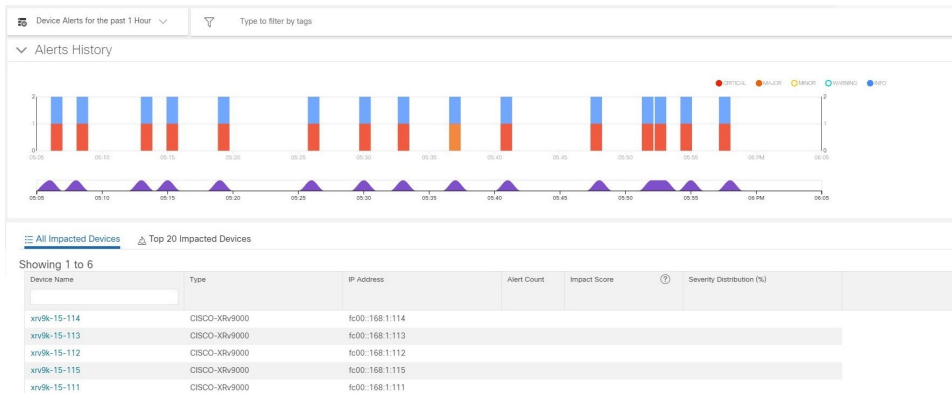
View Alerts for Network Devices

After enabling KPIs on a device, you can view alerts for that device and get data for each performance indicator being monitored.



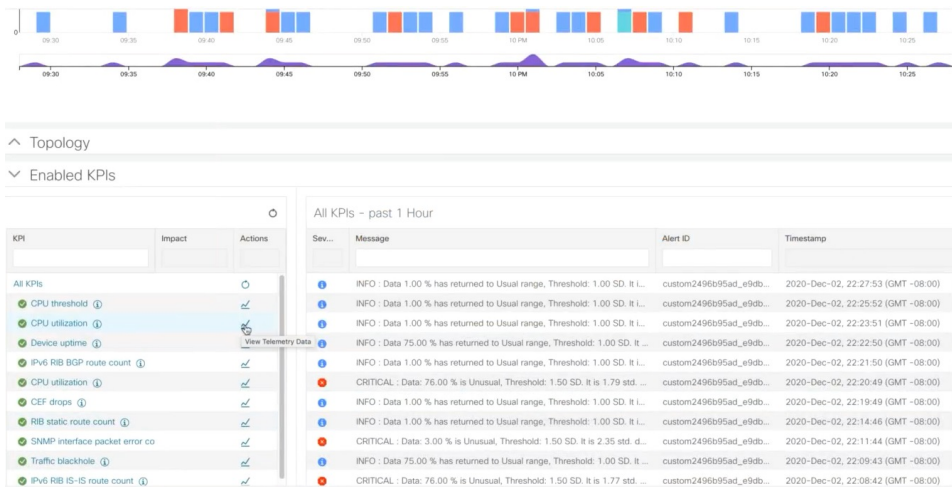
Note The KPIs shown in the following steps are examples. There are many more KPIs available in Health Insights. For the complete list, see [List of Health Insights KPIs, on page 12](#).

Step 1 From the main menu, choose **Performance Alerts > Alert Dashboard**. The Health Insights Alert dashboard is displayed.



Step 2 Make sure that the **Device Alerts** view is displayed (select the **Device Alerts** toggle, if needed). Then scroll down below the **Alert History** panel and click on the **All Impacted Devices** tab. The dashboard displays a list of devices with alerts.

Step 3 Click on the **Device Name** for the device whose details you want to view. Health Insights displays the device's basic **Overview** information, **Alert History**, a **Topology** map, and the list of the device's currently **Enabled KPIs**.



The **Topology** map is a version of the map you see when you select **Topology** from the main menu.

Step 4 Under **Enabled KPIs**, click on the desired KPI to view the detailed KPI information. A graphical representation of that KPIs data, along with a list of alert messages and other information, is displayed on the right.

A graphical time-series representation of the selected KPI is displayed for a 24-hour window with hourly slots.

Step 5 Click on the desired time slot to view the corresponding **Raw** or **Summary** graphical data. Move the mouse cursor over any data point in the graph to view additional popup information for that data point.

Telemetry Data Retention



A red line or tag represents a point at which the KPI was triggered. This can occur on any subscribed statistic the KPI is monitoring. Health Insights collects and identifies the time points and frequency, which help determine when these events become an operational concern.

Note Graphical data is only visible for time slots that has alerts triggered. To view the alerts for the last 24 hours, go to the grafana dashboard (<https://<IPaddress:port>/robot-grafana/>), and select the desired KPI from the dashboard or from the drop-down list. By default, the KPI display is set for last 1 hour. You can change the duration (maximum up to last 24 hours) by selecting the desired option from the drop-down.



Telemetry Data Retention

Telemetry data is collected from devices and stored in the time-series database. This data is retained for one hour, and is used in the Health Insights Alert dashboard to identify alerts using a process known as stream based alerting. The resulting 'alerts', if any, are stored in the same time-series database. The alerts are retained

for 30 days, and the messages showing the duration of alerts are displayed in the top right corner of the Device/KPI view in the Alert dashboard. For more information, see [View Alerts for Network Devices, on page 4](#). The alerts can also be queried using REST APIs.

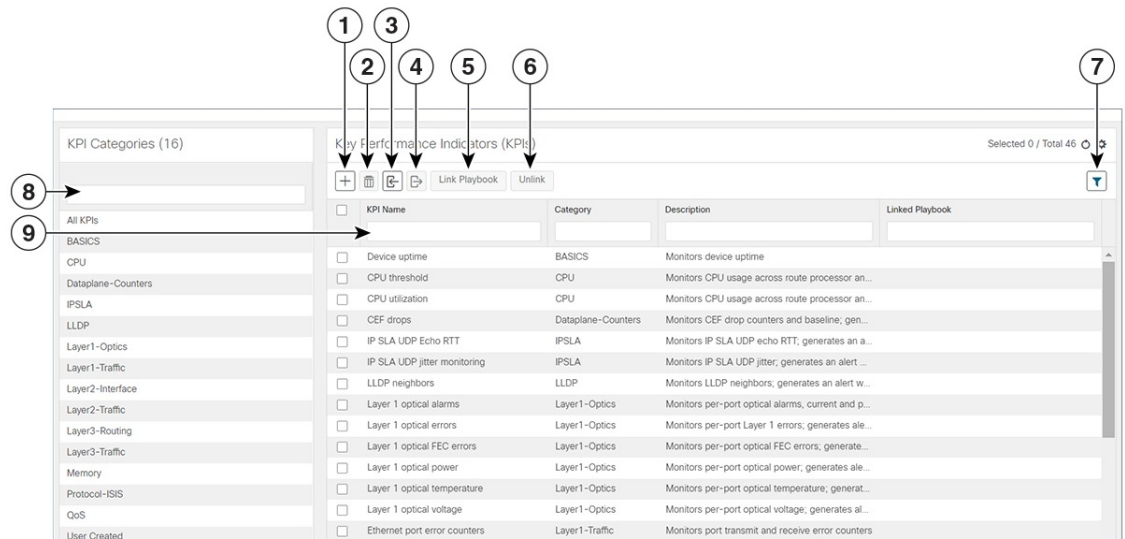


Note The telemetry data displayed in the Alerts dashboard is limited to last only for one hour.






Manage KPIs

The Health Insights Key Performance Indicators (KPI) window gives you complete access to Cisco-supplied and user-created KPIs. You can add, edit, delete, import, and export your KPIs. You can also link your KPIs to the Change Automation application's Playbooks, which enable scripted responses to KPI changes.

To display the Health Insights Manage KPIs window, choose **Performance Alerts > Key Performance Indicators (KPI)** from the main menu.



Item	Description
1	Add KPIs: Click + to add a new, user-created KPI. For help with this task, see Create a New KPI, on page 8 .
2	Delete KPIs: Select one or more existing user-created KPIs in the list and then click 🗑️ . You will be prompted to confirm that you want to delete the KPIs. Click Delete to confirm. Note that you can delete user-created KPIs only. You cannot delete Cisco-supplied KPIs.

Item	Description
3	<p>Import KPIs: Click  to import new user-written or Cisco-supplied KPIs.</p> <p>You will be prompted to browse to the gzipped tar archive containing the KPIs to be imported. When you have selected the archive, click OK to begin importing it. Once imported, the new KPIs will appear immediately in the list of KPIs, with each KPI name and category assigned based on the definition in the KPI itself.</p> <p>In order for Cisco Crosswork Change Automation and Health Insights to import them, KPI files must:</p> <ul style="list-style-type: none"> • Be packaged as a gzip tar archive. You can include more than one KPI in a single archive; each will be imported as a separate KPI. • Have unique names and descriptions. These must not match the name or description of any Cisco-supplied KPI. If the name or description of the KPI matches an existing user-created KPI, the import will overwrite the existing KPI. • Meet other minimum requirements for Health Insights KPIs, as explained in the Cisco Crosswork Network Automation Custom KPI Tutorial Documentation on Cisco DevNet.
4	<p>Export KPIs: Select one or more existing KPIs in the list and then click  to export them. Health Insights will package the exported KPIs as a single TGZ archive with a unique name. Your browser will then prompt you to save the archive to a name and location in your local file system that you select.</p>
5	<p>Link Playbooks: Select a KPI and then click  to link it to a Playbook. That Playbook will execute whenever the KPI raises an alert thereafter. You can specify the values the Playbook will use when operators trigger it in response to the KPI alert. For help with this task, see Link KPIs to Playbooks, on page 10.</p>
6	<p>Unlink Playbooks: Select a KPI with a linked Playbook and then click  to unlink the Playbook. You will be prompted to confirm that you want to unlink the Playbook. Click Unlink to confirm.</p>
7	<p>Clear Filters: Click Clear All Filters to clear any filters you have set.</p>
8	<p>Filter KPI Categories: To find a KPI category, enter all or part of the KPI Category name in this field. Then click  to filter the list below.</p>
9	<p>Filter KPIs: To find a KPI, enter all or part of the KPI Name, Category, Description, or Linked Playbook in the fields provided. The list below is automatically filtered to match your typed entry.</p>

Create a New KPI

You can create a custom KPI and enable it on the desired devices. The workflow is as follows:

1. Supply basic information, such as the KPI name and a summary description.
2. Set the KPI cadence.

3. Select a YANG module and choose sensor paths
4. Select an alert template and set its parameters
5. Enable the KPI on the devices.





Note Health Insights supports creating and using KPIs that will use GNMI as the transport and use sensors based on Open Config (OC) YANG modules for collecting telemetry data (with GNMI transport). The requirements for this feature are:

- GRPC need to be configured in your device.
- The device properties, while onboarding, must mention GNMI under the **Capability** field, and the GNMI protocol details must be provided under the **Connectivity Details** field.
- While creating a KPI, choosing an OC YANG module supports the KPI affinity for GNMI transport, while choosing Cisco-provided YANG models provides the KPI affinity for both MDT and GNMI transports.

The GNMI transport capability is determined at runtime based on the the following factors such as GNMI capability of the device, GNMI affinity of the KPI, and the combined capability as a set of devices in a KPI Profile.

The following steps explain how to create a KPI:

-
- Step 1** From the main menu, choose **Performance Alerts > Key Performance Indicators (KPI)**. The **Key Performance Indicators (KPI)** window is displayed.
- Step 2** Click the . The **Create KPI** window opens.
- Step 3** In the text fields provided, enter a unique **KPI Name**, a short **KPI Summary** description, and **KPI details**. The **KPI Group** is preset to `User Created`.
- Step 4** The **Cadence** field sets the number of times per minute the KPI will gather sensor data from the devices on which the KPI is enabled. Leave it at the default or use the numerical selector to choose a different value.
- Step 5** In the **YANG Modules** area, choose one module and one or more sensor paths from which to stream data:
- a) Use the **Module** field to filter and choose the desired Cisco IOS XR YANG module.
 - b) Use the table fields to filter and choose the desired sensor path. When you choose a path, the leaf node gets resolved to the base encoding path. If the YANG module is hierarchical, the field names are concatenated down from the base path. Note that only one gather path is supported for user-created KPIs.
- Click **Next** to display the **Select Alert Templates** window.
- Step 6** Choose the alert template you want to use with your new KPI: **No Alert**, **Standard Deviation**, **Two-Level Threshold** or **Rate Change**. Then click **Next** to display the **Alert Parameters** window appropriate for the type of alert template you chose.
- Step 7** Edit the alert template parameter values as appropriate for the template and the purpose of your KPI, as follows:
- Use the **Basic** and **Advanced Parameters** dropdowns to view and edit the parameter sets you need.
 - Change alert parameter numerical values using the selectors or by editing the field contents
 - Change alert parameters with discrete choices using parameter field dropdowns and select each choice as needed.
 - Learn more about an alert parameter: Hover your mouse cursor over the  shown next to the parameter name.

- Click the **View Tick Script** link to view the tick script code you are generating with your changes. The tick script code updates as you make your edits. At any time, click the **Hide Tick Script** to close the tick script code window.

Step 8 When you are finished making changes, click **Finish** to save the new KPI and display the **Key Performance Indicators (KPI)** window.

Link KPIs to Playbooks

You can link any Health Insights KPI to one Change Automation Playbook of your choice. A user can run the linked Playbook whenever the linked KPI raises an alert in response to the event associated with the performance indicator the KPI is monitoring. The KPI alert can be raised in response to a threshold crossing, topology changes, flapping conditions, and other parameters. These parameters will vary, as appropriate, for each KPI.



Note This procedure is not applicable if the Change Automation application is not installed in your device. In this case, the UI features that link Health Insights and Change Automation (e.g. Link Playbook) are not displayed in the UI.

You can specify the **Source** of the parameter values the linked Playbook will use when you run it. You can select these sources:

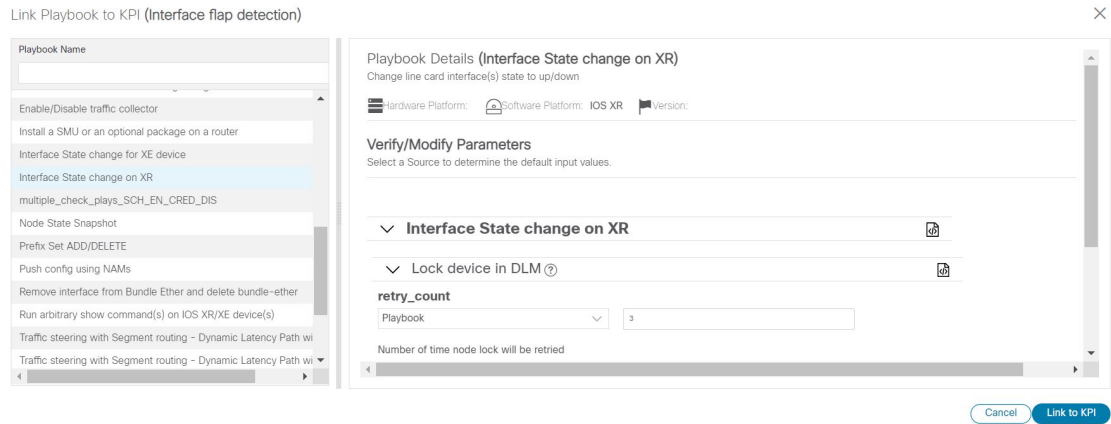
- **Playbook:** Use default values coded into the Playbook itself
- **KPI Alert:** Use values taken from the alert raised by the linked KPI.
- **Runtime Input:** Use values you enter only at the moment you run the Playbook.

The ability to set the source of these Playbook parameter values gives you flexibility in how you use the linked Playbook. For example: Link the KPI **Interface flap detection**, which detects interface flapping, to the Playbook **Interface state change on XR**, which can be used to set the interface up or down. Depending on circumstances, you might want to set the Playbook parameters as follows:

- **Playbook:** You want to run the Playbook as it normally does, so you would set the **Source** as **Playbook** for the *provider*, *collection_type* and *mop_timeout* parameters. In the case of the *collection_type*, you can still choose between **telemetry** and **snmp**, depending on whether you want to use MDT or SNMP to gather device data.
- **KPI Alert:** You want the Playbook to run only on the host device and interface affected by the flapping, which are identified in the flap-detection Alert. So set the **Source** of the Playbook's *hosts* and *if_names* parameters to **KPI Alert**. You can then use the alert's data about the **Producer** device and the **interface_name** of the flapping interface on that device.
- **Runtime Input:** You want the freedom to decide at runtime whether to bring the flapping interface up or down. So set the **Source** of the Playbook parameter *admin_state* to **Runtime Input**. The Playbook will prompt you for an **up** or **down** choice when you initiate the run.

The following figure shows what this set of choices will look like:

Figure 1: Example: Specifying Parameter Value Sources for a Linked Playbook



- Step 1** From the main menu, choose **Performance Alerts > Key Performance Indicators (KPI)**. The **Key Performance Indicators (KPI)** window opens, displaying lists of the KPI categories and the KPIs available in each category.
- Step 2** Select the KPI you want to link to a Playbook. You can use filters to find the KPI you want, as explained in [Manage KPIs, on page 7](#).
- Step 3** Click [Link Playbook](#). The **Link Playbook to KPI** window opens.
- Step 4** The left side of the window lists the name of the selected KPI and the Playbooks appropriate for linking to it. Scroll through the list, or use the **Playbook Name** field to restrict the list to just the Playbooks you want.
- Step 5** When you have found the Playbook you want to link, click on its name. The right side of the window will then list the **Playbook Details** for the selected Playbook, including:
- The hardware and software platforms with which it is compatible.
 - The minimum software version requirement
 - The **Source** and default values that will be used when the Playbook runs. In many cases, you can select from a range of default values, or enter your own.
- Step 6** Verify or modify the **Source** and parameter values as needed.
- Step 7** When you are finished making changes, click **Link to KPI**. The **Key Performance Indicators (KPI)** window is displayed again, this time with the linked Playbook shown next to name of the KPI in the **Key Performance Indicators (KPIs)** list.
- Step 8** To change the Playbook linked to a given KPI, repeat steps 3 through 7 for that KPI, this time choosing the Playbook you want. To unlink a Playbook entirely, select the KPI and click [Unlink](#).

Verify the Deployment Status of Enabled KPIs

After you enable a KPI Profile, you can verify the deployment status.

-
- Step 1** From the main menu, choose **Performance Alerts > KPI Job History**. The **KPI Job History** window lists the jobs that have been run most recently, indicating whether they succeeded or failed, when they ran, and on what devices.
- Step 2** Click the transaction ID in the job listing to view detailed KPI job information, including the device on which the KPI Profile was enabled and the KPI ID.
-

List of Health Insights KPIs

The table below lists the prebuilt Health Insights KPIs supplied with Cisco Crosswork Change Automation and Health Insights.

Alerting types in the table that you can select when you create a new KPI (see [Create a New KPI, on page 8](#)) are:

- **No Alert:** The KPI gathers, tracks and reports performance data without triggering alerts.
- **Standard Deviation:** The KPI detects spikes or drops in measured values and alerts when these values deviate some number of standard deviations away from their normal values.
- **Two-Level Threshold:** The KPI detects abnormal measured values using two custom thresholds and the ability to provide dampening intervals on the thresholds.
- **Rate Change:** The KPI detects abnormal rates of change in measured values to detect rising or falling values.

Additional alerting types that you can use when you export and use a prebuilt KPIs to create KPIs with custom parameters are:

- **Standard Deviation of Rate Change:** The KPI alerts on standard deviations of the rate of change.
- **Low Single Threshold:** The KPI alerts on a single threshold when the value falls below that threshold.
- **Direct Alarm Forwarding:** The KPI uses the alarm from the device directly, as a Health Insights KPI alert.
- **Major/Minor/Low/High Thresholds:** The KPI alerts on Major high, Minor high, Minor low, and Major low values.
- **Line State Changes:** The KPI alerts on shutdowns and flapping in line states.

For more on creating KPIs with custom parameters from exported KPIs, see the [Cisco Crosswork Network Automation Custom KPI Tutorial Documentation on Cisco DevNet](#).

Table 1: Health Insights KPIs

Category	KPI Name	Description	Alerting	Protocol
Dataplane-Counters	CEF drops	Monitors CEF drop counters and baseline. Generates an alert for an unusual number of drops.	Rate Change	MDT, GNMI

Category	KPI Name	Description	Alerting	Protocol
CPU	CPU threshold	Monitors CPU usage across route policies and line cards on routers. Generates an alert when CPU utilization exceeds the configured threshold	Two-Level Threshold	MDT, GNMI
CPU	CPU utilization	Monitors CPU usage across route policies and line cards on routers. Generates an alert when CPU utilization is unusual.	Standard Deviation	MDT, GNMI
Basics	Device uptime	Monitors device uptime.	Low Single Threshold	MDT, GNMI
Layer 1-Traffic	Ethernet port error counters	Monitors port transmit and receive error counters.	Rate Change	MDT, GNMI
Layer 1-Traffic	Ethernet port packet size distribution	Monitors port transmit and receive packet size distributions.	No Alert	MDT, GNMI
Layer 1-Traffic	Ethernet port packet statistics	Monitors port transmit and receive packet statistics.	Standard Deviation of Rate Change	MDT, GNMI
Layer 2-Traffic	Interface bandwidth monitor	Monitors bandwidth utilization across all interfaces on a router. Generates an alert when bandwidth exceeds the configured threshold.	Two-Level Threshold	MDT, GNMI
Layer 3-Traffic	Interface counters by protocol	Monitors interface statistics (such as incoming and outgoing packets or byte counters) organized by protocol.	Standard Deviation	MDT, GNMI
Layer2-Interface	Interface flap detection	Monitors interface flaps and alerts when flap count reaches set threshold.	Two-Level Threshold	MDT, GNMI
Layer 2-Traffic	Interface packet counters	Monitors interface transmit and receive counters. Generates an alert when unusual traffic rates occur.	No Alert	MDT, GNMI
Layer 2-Traffic	Interface packet error counters	Monitors interface transmit and receive error counters. Generates an alert when unusual error rates occur.	Rate Change	MDT, GNMI
QOS	Interface QoS (egress)	Monitors interface QoS on the egress direction for queue statistics, queue depth, and so on.	No Alert	MDT, GNMI
QOS	Interface QoS (ingress)	Monitors interface QoS on the ingress direction for queue statistics, queue depth, and so on.	No Alert	MDT, GNMI

Category	KPI Name	Description	Alerting	Protocol
Layer 2-Traffic	Interface rate counters	Monitors interface statistics as rate counters. Generates an alert when unusual traffic rates occur.	Standard Deviation	MDT, GNMI
IPSLA	IP SLA UDP echo RTT	Monitors IP SLA UDP echo RTT. Generates an alert when unusual RTT values occur.	Standard Deviation	MDT, GNMI
IPSLA	IP SLA UDP jitter monitoring	Monitors IP SLA UDP jitter. Generates an alert when an abnormal UDP jitter occurs.	Standard Deviation	MDT, GNMI
Layer 3-Routing	IPv6 RIB BGP route count	Monitors IPv6 RIB for route count and memory used by BGP. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIB IS-IS route count	Monitors RIB for route count and memory used by IS-IS. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	IPv6 RIB IS-IS route count	Monitors IPv6 RIB for route count and memory used by IS-IS. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	IPv6 RIB OSPF route count	Monitors IPv6 RIB for route count and memory used by OSPF. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Protocol-ISIS	ISIS neighbor summary	Monitors ISIS neighbor summaries for changes in neighbor status. Generates an alert when an anomaly is detected (such as neighbors down or flapping).	Standard Deviation	MDT, GNMI
Layer 1-Optics	Layer 1 optical alarms	Monitors per-port optical alarms (current and past).	Direct Alarm Forwarding	MDT, GNMI
Layer 1-Optics	Layer 1 optical errors	Monitors per-port Layer 1 errors. Generates an alert when error rates exceed the configured threshold.	Rate Change	MDT, GNMI
Layer 1-Optics	Layer 1 optical FEC errors	Monitors per-port optical FEC errors. Generates an alert when FEC errors exceed the configured threshold.	Rate Change	MDT, GNMI

Category	KPI Name	Description	Alerting	Protocol
Layer 1-Optics	Layer 1 optical power	Monitors per-port optical power. Generates an alert when power levels exceed the configured threshold.	Major/Minor/Low/High Thresholds	MDT, GNMI
Layer 1-Optics	Layer 1 optical temperature	Monitors per-port optical temperature. Generates an alert when temperature exceeds the configured threshold.	Major/Minor/Low/High Thresholds	MDT, GNMI
Layer 1-Optics	Layer 1 optical voltage	Monitors per-port optical voltage. Generates an alert when voltages exceed the configured threshold.	Major/Minor/Low/High Thresholds	MDT, GNMI
Layer 2-Interface	Line state	Monitors interface line states. Generates an alert when link states change.	Line State Changes	MDT, GNMI
LLDP	LLDP neighbors	Monitors LLDP neighbors. Generates an alert when any sudden changes are detected.	Standard Deviation	MDT, GNMI
Memory	Memory utilization	Monitors memory usage across route processor and line cards on routers. Generates an alert when memory utilization is unusual.	Standard Deviation	MDT, GNMI
Memory	Memory utilization (cXR)	Monitors memory usage across route processor and line cards on classic XR devices. Generates an alert when memory utilization is unusual.	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIB BGP route count	Monitors RIB for route count and memory used by BGP. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIB connected route count	Monitors RIB for route count and memory used by connected. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIB IS-IS route count	Monitors RIB for route count and memory used by IS-IS. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts)	Standard Deviation	MDT, GNMI

Category	KPI Name	Description	Alerting	Protocol
Layer 3-Routing	RIB local route count	Monitors RIB for route count and memory used by local. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIB OSPF route count	Monitors RIB for route count and memory used by OSPF. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIB static route count	Monitors RIB for route count and memory used by static. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIPv6 connected route count	Monitors RIPv6 for route count and memory used by connected. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIPv6 local route count	Monitors RIPv6 for route count and memory used by local. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIPv6 static route count	Monitors RIPv6 for route count and memory used by static. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 3-Routing	RIPv6 subscriber route count	Monitors RIPv6 for route count and memory used by subscriber. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, GNMI
Layer 2-Traffic	SNMP interface packet error counters	Monitors interface transmit and receive error counters. Generates an alert when unusual error rates occur.	No Alert	SNMP
Layer 2-Traffic	SNMP interface packet counters	Monitors interface transmit and receive counters. Generates an alert when unusual traffic rates occur.	Rate Change	SNMP

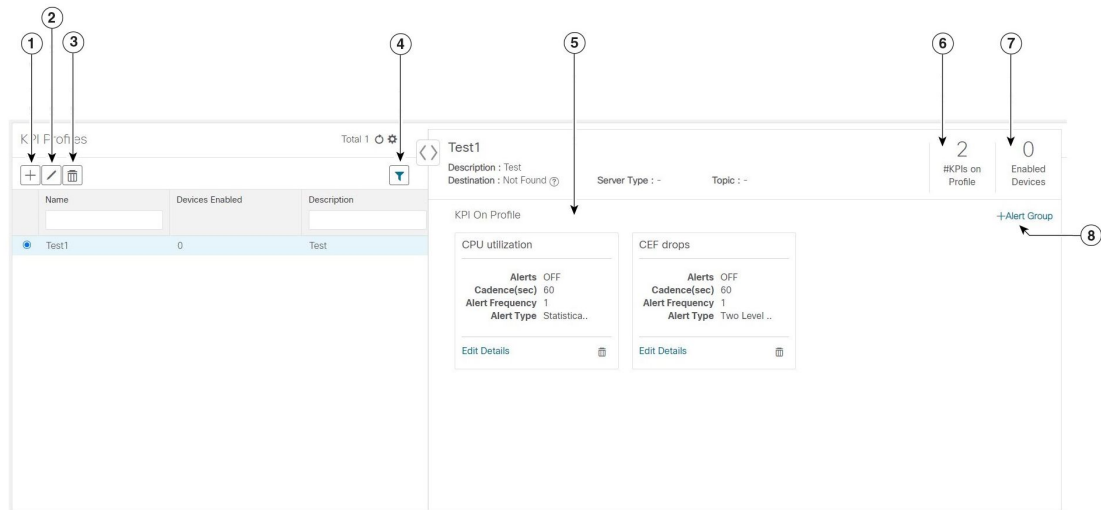
Category	KPI Name	Description	Alerting	Protocol
Layer 2-Traffic	SNMP interface rate counters	Monitors interface statistics as rate counters. Generates an alert when unusual traffic rates occur.	Standard Deviation Rate of Change	SNMP
Layer 2-Traffic	SNMP traffic black hole	Monitors input and output data rates for black hole behavior. Checks the ratio of output data rate to input data rate and verifies that the ratio is within acceptable ranges, otherwise a black hole is occurring.	Two-Level Threshold	SNMP
Layer 2-Traffic	Traffic black hole	Monitors input and output data rates for black hole behavior. Checks the ratio of output data rate to input data rate and verifies that the ratio is within acceptable ranges, otherwise black hole.	Two-Level Threshold	MDT, GNMI
Layer 2-Traffic	Interface packet error counters (Openconfig)	Monitors interface error counters; generates an alert when unusual error rates occur. This KPI uses openconfig-interfaces YANG model.	Rate Change	GNMI
Layer 2-Traffic	Interface rate counters (Openconfig)	Monitors interface statistics (such as rate counters), and generates an alert when unusual traffic rates occur.	Rate Change	GNMI
File System	Filesystem Utilization	Monitors filesystem usage on active route processor and generates an alert when filesystem utilization exceeds the configured threshold.	Two-Level Threshold	CLI

Manage KPI Profiles

The Health Insights KPI Profiles window allows you to create, edit, and delete KPI Profiles.

A KPI Profile is a collection of KPIs and their corresponding parameters such as alert frequency, alert type, cadence, and more. You can group relevant KPIs into a KPI Profile, give it meaningful name based on the purpose (for example, environmental or health check), and configure parameters that are relevant to monitoring a specific type of devices (for example, edge routers). Once the KPI profiles are created and validated by the system, they are ready to be used. You can select the device(s) in Health Insights, select appropriate KPI Profiles and enable them. This action enables all the KPIs in the selected KPI Profile. Similarly, you can select the device(s) and choose to disable the KPI Profiles. This removes all KPIs enabled as part of the selected KPI profile(s) from the devices (for MDT based KPIs) and the collection jobs for the KPIs on the CDG.

To display the Health Insights KPI Profiles window, choose **Performance Alerts > KPI Profiles** from the main menu.



Item	Description
1	Create KPI Profile: Click <input type="button" value="+"/> to create a new, user-created KPI Profile. For help with this task, see Create a New KPI Profile, on page 18 .
2	Edit KPI Profile: Select a user-created KPI Profile in the list and then click <input type="button" value="✎"/> to edit it. For help with this task, see Create a New KPI Profile, on page 18 .
3	Delete KPI Profile: Select a user-created KPI Profile in the list and then click <input type="button" value="🗑️"/> to delete it. You cannot delete a KPI Profile that has been enabled on any device(s).
4	Filter KPI Profile: To find a KPI category, enter all or part of the KPI Profile name in this field, and the list is automatically filtered based on your input. Click <input type="button" value="✕"/> to clear any filters you have set.
5	KPI On Profile: The KPI(s) added on the selected KPI Profile and the associated parameters are displayed here. You can edit the KPI parameters, or remove a KPI from the selected KPI Profile using the appropriate options here.
6	#KPIs on Profile: This is the number of KPIs added on the selected KPI Profile.
7	Enabled Devices: This is the number of devices on which the selected KPI Profile is enabled.
8	+Alert Group: Click this option to create Alert Group for the selected KPI Profile. For help with this task, see Create a New KPI Profile, on page 18


Create a New KPI Profile


You can create a KPI Profile and enable it on the desired devices. The workflow is as follows:

1. Supply basic information, such as the Profile name and a description.
2. Add KPI(s) and save the profile.
3. Edit KPI parameters and create alert groups.

4. Enable the KPI Profile on the devices.

The following steps explain how to perform all of these tasks.

-
- Step 1** From the main menu, choose **Performance Alerts > KPI Profiles**. The **KPI Profiles** window is displayed.
- Step 2** Click the . The **Create New Profile** window is displayed.
- Step 3** In the text fields provided, enter a unique **Profile Name**, a short **Description**. The **Profile Name** can contain a maximum of 32 alphanumeric characters, plus underscores ("_"). No other special characters are allowed.
- Step 4** (Optional) You can specify an external destination to send the data collected by KPIs. To create an external data destination, go to **Administration > Data Gateway Global Settings** Provide relevant values for the following fields:
- **Server Type**: Select either KAFKA or GRPC.
 - **Name**: Select the name of the external destination.
 - **Topic**: Enter a topic to provide context for the data being sent. This field is applicable only for KAFKA.
- Note** You need to create a new data destination to export the KPI data. The predefined data destinations cannot be used for this activity. For more information about creating a data destination, see the *Cisco Crosswork Infrastructure 4.0 and Applications Administration Guide*.
- Step 5** Add KPI to the profile, using the following filter options:
- a) **All KPIs**: By default, this option is selected and the list of all KPIs are displayed in the list. You can select the required KPI by checking the relevant checkbox.
 - b) **Recommended KPIs**: You can select KPIs based on the KPIs recommended for a specific device. Click **Recommended KPIs** and the device list is displayed. You can filter the device list by entering relevant values in the Name field, or by using tags. Select a device from the list and the recommended KPI list is displayed on the right side. Select the required KPI by checking the relevant checkbox.
- Note** Selecting KPIs from the recommended KPI list of a selected device does not automatically enable the KPI Profile in the selected device. The KPI Profile can be enabled after it is created. For more information, see [Enable KPI Profile on Devices, on page 21](#)
- Step 6** Click **Save** save the new KPI Profile and display the **KPI Profiles** window.
- Step 7** In the **KPI Profiles** area on the left side, choose the KPI Profile that you created, and the individual KPI details are displayed on the right side.
- Step 8** You can leave the KPI parameters at the default or choose a different value. To edit the KPI parameters, click **Edit Details**, and the **KPI Details** window is displayed. Edit the parameter values as appropriate for the purpose of your KPI. The common parameters are:
- **Alert**: This is an on/off toggle switch for alerting. Based on the **Alert** parameter value, the corresponding alerting logic is deployed. Alerting can be enabled even after the KPI Profile has been applied to the devices.
- Note** Any KPI using the composite alerting logic need to have the alerting flag set to ON.
- **Cadence (sec)**: Set the frequency of sensor data. Set the frequency (in seconds) in which the KPI will gather sensor data from the devices on which the KPI Profile is enabled.
 - **Alerting Down Sample Rate**: Alert frequency rate. It determines how often KPI data will be evaluated for any alert conditions, and is relative to the Cadence. For example, if Cadence is 60 seconds and you want to do an alerting evaluation every 300 sec, then specify Alerting Down Sample Rate as "5".

Step 9 You can also edit the alert logic parameters of the selected KPI. To learn more about a parameter, hover your mouse cursor over the  shown next to the parameter name.

Note When different thresholds are desired for different types of devices in the network, it is advisable to create multiple profiles and split the KPIs across them to meet the needs of different device types.

Step 10 When you are finished making changes, click **Save** to save the new KPI Profile. Health Insights validates your input parameters and displays the **KPI Profiles** window.

Note You can create up to 50 KPI profiles, and an individual KPI Profile can consist up to 50 KPIs. KPI profile creation can fail if the total number is exceeded, or if Health Insights could not create the required tags in Inventory manager. This status is reflected in the profile state. Once profile is ready, it can be applied on devices.

With the **KPI Profiles** window displayed, you can enable the new KPI Profiles on one or more devices immediately, following the steps given in [Enable KPI Profile on Devices, on page 21](#).

See [Disable KPI Profile on Devices or Device Groups, on page 23](#) for instructions to disable KPI Profiles.

Step 11 (Optional) You can also create alert groups for a KPI Profile. Alert groups use boolean logic (cascaded OR and AND) to combine alert outputs from primary KPIs in your KPI profile and create a composite logic query. To create an alert group, click + **Alert Group**. The **Create Alert Group** window is displayed.

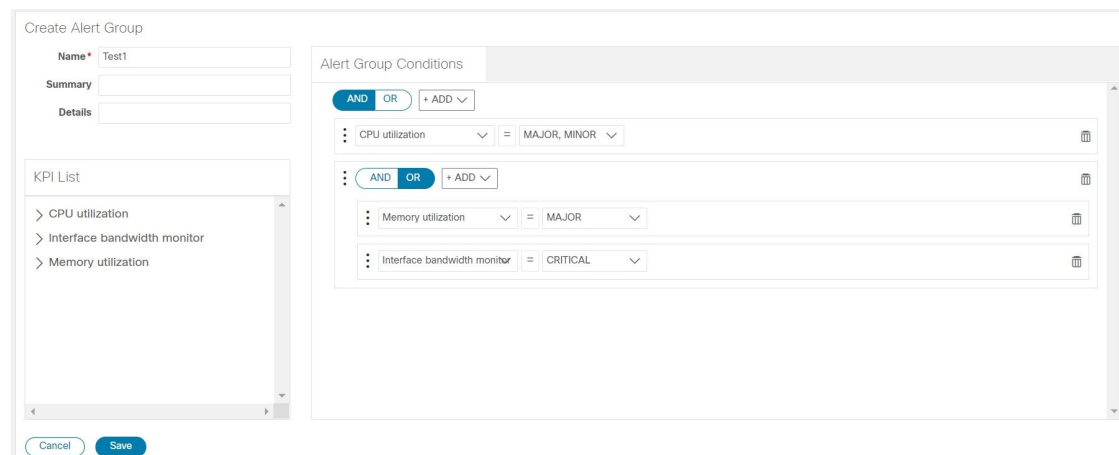
Note Configuring an alert provider enables composite alert forwarding.

Step 12 Provide a relevant entry in the **Name** field. **Summary** and **Details** are optional fields.

Step 13 The **Alert Group Conditions** area on the right side lets you select a logic gate (AND/OR) and add a KPI on which the logic is applied. Your alert group can be based on the alert criteria of a single KPI, or it can be a combination of multiple KPI outputs. Click the desired logic (**AND** gate is selected by default), and click the + **ADD** dropdown list to add an **Item** or a **Group**.


Item allows you to add individual KPI items and set the corresponding alert level, and **Group** allows you to add a nested alert group.

Step 14 Choose the desired KPI from the **Select KPI** dropdown, and select the desired level(s) for which the alerts need to be set for the chosen KPI. The alert levels are CRITICAL, MAJOR, MINOR, WARNING and INFO. Based on the logic gate and alert criteria you select, the output of the KPIs are evaluated and the alert is generated.



The screenshot shows the 'Create Alert Group' window. On the left, there are input fields for 'Name' (containing 'Test1'), 'Summary', and 'Details'. Below these is a 'KPI List' with three items: 'CPU utilization', 'Interface bandwidth monitor', and 'Memory utilization'. On the right, the 'Alert Group Conditions' section shows a logic gate set to 'AND' and three conditions: 'CPU utilization = MAJOR, MINOR', 'Memory utilization = MAJOR', and 'Interface bandwidth monitor = CRITICAL'. At the bottom, there are 'Cancel' and 'Save' buttons.

In the example shown above, the alert is set based on the output of two logic gates. The first logic gate is the output of an **OR** operation between the **Memory Utilization** and **Interface Bandwidth monitor** KPIs. If the set alert levels are met for either of the KPIs, the output of the first logic gate is set as true. This output is considered as the input for the second logic gate, which is an **AND** operation with the **CPU Utilization** KPI. If the alert levels of both the KPIs are met, the output of the second logic gate is set as true.

Step 15 Click **Save** to save the new alert group and display the **KPI Profiles** window. Click **Edit Details** or  to edit or delete an existing alert group respectively.

Enable KPI Profile on Devices

With Health Insights, you can enable and monitor the KPI Profiles in which you are interested. Instead of sifting through all the data that a given device can supply, you choose to monitor only the information relevant to the role the device plays in your network. Your equipment and management infrastructure operates as efficiently as possible, without requiring the collection and storage of data that is unrelated to device roles. This operational efficiency reduces the amount of time required to set up specific monitoring, leading to faster problem identification and resolution.

Note that some KPIs trigger alerts based on deviation from an established level of performance. For these types of KPIs, it is necessary to allow the system some annealing time in order to establish normal performance levels.



Important You can only enable KPI Profiles with MDT-based KPIs on a device that has been mapped to a Cisco Network Services Orchestrator (Cisco NSO) provider and attached to a Crosswork Data Gateway.




Note Do not enable KPI Profiles on devices that are not reachable, as it will likely result in a timeout.

To enable KPI Profile on devices:

Step 1 From the main menu, choose **Performance Alerts > Enable/Disable KPI Profiles**. The **Devices** window is displayed.

Step 2 Select the devices for which you want to enable KPI Profiles. You can click the **Device** or **Device Tags** buttons above the table on the left to toggle between selecting the devices by name or by tagged device group membership. Depending on your selection, the device list or the device tag list is displayed on the left.

If you choose to select by **Device**:

- Click  in the table on the right. Type a **Name** or **Device Type** in the filter fields. As you type, the table displays only the devices whose name or type match the text you typed.
- Click the check box next to the device(s) you want. You can select multiple devices at the same time.

If you choose to select by **Device Tags**:

- Type a tag name in the **Name** field to find a Device Group in the table. As you type, the table displays only the tag names that match the text you typed.

- Click the check box next to the group you want. The names of all the devices in that group appear in the devices table on the right.

Select by Devices Device Tags

Devices Selected 7 / Total 20

Enable KPI Profiles Disable KPI Profiles

	Reachability	Name	Device Type	Operational State	Enabled Profiles
<input type="checkbox"/>		spnac-a9k-s077	ROUTER		
<input checked="" type="checkbox"/>		spnac-a9k-s078	ROUTER		
<input checked="" type="checkbox"/>		cw1-r66	ROUTER		
<input checked="" type="checkbox"/>		cw1-r67	ROUTER		
<input checked="" type="checkbox"/>		cw1-r69	ROUTER		
<input checked="" type="checkbox"/>		spnac-a9k-s080	ROUTER		
<input checked="" type="checkbox"/>		cw1-r63	ROUTER		
<input checked="" type="checkbox"/>		cw1-r70	ROUTER		
<input type="checkbox"/>		spnac-a9k-s079	ROUTER		
<input type="checkbox"/>		cw1-r61	ROUTER		
<input type="checkbox"/>		spnac-a9k-s074	ROUTER		
<input type="checkbox"/>		spnac-a9k-s075	ROUTER		

Step 3 Click **Enable KPI Profiles** to continue. Health Insights detects the selected devices, their types and models, and retrieves and analyzes their running configurations. The **KPI Profiles** window presents the KPI Profiles available for your selected devices.

Step 4 Choose the KPI Profiles you want to enable by clicking the check box next to the KPI Profile name, and click **Next**. The **Verify Details** window appears, listing all the KPI Profiles you have chosen to be enabled on the selected devices.

Step 5 (Optional) To get information about the KPIs included in the KPI Profile. Click the KPI Profile in the **Selected Profile(s)** table, and the content of the selected KPI Profile is displayed on the right side. Click **View More Details** to view the parameters of a specific KPI. A popup window provides the details of the KPI. Click the **X** to close the popup window.

Step 6 To enable the selected KPI Profiles on the selected devices, click **Enable**. Health Insights schedules the KPI Profile(s) as a series of job sets.

Note The **Alert** flag for the KPI profile (click **Edit Details** on the relevant KPI) must be turned **ON** in order to trigger an alert when the data is collected.

Note Enabling a KPI results in configuration of the devices (for MDT-based KPIs) and the Crosswork Data Gateway attached to the device, to receive and forward the reported data. For SNMP-based KPIs, the Crosswork Data Gateway will be configured to poll and collect the data, and forward it to Health Insights for processing and evaluation.

Step 7 From the main menu, choose **Performance Alerts > KPI Job History** to watch the progress of each job set, as shown below. You should see job sets completing with a status of "Success". If job sets complete with a "Partial" or "Failed" status, be sure to read the job completion messages, and check that the selected devices are still reachable.

Job Sets			Job Details			
State	Job Set ID	Start Time	Job Set ID	Status	Start Time	End Time
	0002	11/27/2019 10:42:38	0001	Job Completed	Wed Nov 27 2019 10:41:23 GMT+5:30	Wed Nov 27 2019 10:42:13 GMT+5:30
	0001	11/27/2019 10:41:23		0 Failures		

Jobs (2)					
Status	Operation	KPIs or *Alert Group	KPI Profile	Device	Message
	Create	pulse_cef_drops	Test1	cw1-r66	
	Create	pulse_cpu_utilization	Test1	cw1-r66	

When the job sets complete successfully, the KPIs are now associated to the devices and the platform begins the process of enabling the relevant collection procedures for those network elements. In making these changes, you are automating the configuration of both the platform and the devices themselves to collect only the information required.

- Step 8** From the main menu, choose **Performance Alerts > Alert Dashboard**. The dashboard shows the alert status for the devices on which you have enabled KPI monitoring.

**Note**

- SNMP/MDT jobs may take more time than expected to reach the completed state when there is an increase in the number of devices, interfaces and KPIs.
- Enabling KPI profile per device takes around 3 to 5 seconds. If the device is not reachable, it will keep trying until it is timed out. This may result in the job taking more time to reach the completed state.

Disable KPI Profile on Devices or Device Groups

You can use the **Enable/Disable KPI Profiles** window to disable the KPI Profiles running on device(s) or device groups.

- Step 1** From the main menu, choose **Performance Alerts > Enable/Disable KPI Profiles**. The **Enable/Disable KPI Profiles** window is displayed.
- Step 2** To disable KPIs enabled on one or more devices:
- a) Click the **Device** button above the table on the left. The **Devices** table displays all the devices, with the total number of KPIs enabled on each device.
 - b) Click the checkbox next to the devices on which you want to disable KPIs.

If you select one device, you can disable all KPI Profiles for the device or just some of the KPI Profiles. If you select more than one device, you can only disable all KPIs for them.
 - c) Click **Disable KPI Profiles**. You will be prompted to confirm that you want to disable the KPIs running on all the selected devices. If you selected only one device, click the checkboxes next to the KPI Profiles you want to disable on that device, or click the checkbox at the top of the column to disable all the KPI Profiles running on that device. Click **Disable** to confirm.
- Step 3** To disable all KPI Profiles enabled on all the devices within a device group:
- a) Click the **Device Tags** button above the table on the left. The table displays the list of device tags.
 - b) Click the checkbox next to the device tag(s) on which you want to disable KPI Profiles.

When you select a device tag, the **Devices** table on the right shows all the devices that are associated with that tag. All of the devices are preselected.
 - c) Click **Disable KPI Profiles**. You will be prompted to confirm that you want to disable all the KPIs running on all the devices in the group. Click **Disable** to confirm.

Troubleshoot Health Insights

The following table describes issues you may encounter when using the Health Insights application, and their solutions or workarounds.

Table 2: Health Insights Troubleshooting

Issue	Solution
Apply a KPI to a device fails with messages indicating that Cisco Network Services Orchestrator (Cisco NSO) and the target device are out of sync or otherwise out of communication. Message text will vary, but may include "device out of sync", "NC client timeout", and other text indicating that there are connectivity or sync issues between NSO and the device.	Apply the KPI again. Under normal circumstances, doing so will initiate a sync operation between the device and NSO.
Health Insights not receiving data.	<ol style="list-style-type: none"> 1. Confirm that the KPI configuration job completed without error: Go to Performance Alerts > KPI Job History 2. Check the Collection/distribution status: Go to Administration > Collection Jobs.