Monitor Network Health and KPIs

This section contains the following topics:

Health Insights overview

Health Insights is a network health application that:

- performs real-time key performance indicator (KPI) monitoring, analytics, and alerting and aids in troubleshooting.

- builds dynamic detection and analytics modules that allow operators to monitor and alert network events with user-defined logic.

- provides prebuilt KPIs that are based on Model-Driven Telemetry (MDT), SNMP-based telemetry, or GNMI/Openconfig based telemetry collection.

The Health Insights Recommendation Engine uses data mining to analyze your network and recommends which telemetry paths you should enable and monitor.

Note For MDT-based KPIs, Crossword Network Controller pushes the KPI configuration down to the device. For SNMP, CLI, and GNMI-based KPIs, the operator must have the device configured to respond to a request for telemetry data.

Important Due to the additional data collection tasks required, Health Insights requires the use of extended Data Gateways.

The following high-level example gives a basic view of how Health Insights interacts with the other Crosswork Network Controller 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.

Health Insights is configured to gather the link bandwidth usage data for device links. After a time period, it establishes a performance baseline for each link. If a link deviates from its baseline causing an alert to be generated, Health Insights detects it and you can then go and run the Playbook to reconfigure the network to resolve the issue.

The complexity of the interaction will depend on the type of anomaly, how it is detected, and the playbooks you choose to use to remediate it. You can orchestrate any form of network remediation using Change Automation playbooks, helping you to close the loop on problem resolution and maximize network performance.

Health Insights collects telemetry data from devices and stores it for the last 72 hours in a time-series database. This data is used for real-time KPI monitoring, analytics, and generating alerts. Triggered alerts are stored and retained for 30 days in the same database, and the messages showing the alerts' duration are displayed at the top of the Device/KPI view in the Alert dashboard.

List of Health Insights KPIs

This section lists the prebuilt Health Insights KPIs supplied with Health Insights application.

Supported protocols

The target device(s) must support the form of telemetry used by the KPI either SNMP, GNMI, or MDT. The application validates for a match between KPI and device telemetry capabilities.

Definition of the protocols:

- Model-Driven Telemetry (MDT): Model-driven telemetry provides a mechanism to stream operational data from device as defined in the YANG model(s) to a data collector.

- gRPC Network Management Interface (gNMI): gNMI provides the mechanism to install, manipulate, and delete the configuration of network devices, and also to view operational data.

- Simple Network Management Protocol (SNMP): SNMP is an IP protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

- Command Line Interface (CLI): CLI is used in network device management.

Health Insights uses either MDT or gNMI protocols but the device supports both. gNMI is a preferred default.

Note In Crosswork Network Controller version 7.1, new sensor paths have been introduced for the Layer3-Routing, QoS, and Layer2-Traffic (Opencofig-interfaces) KPI categories to ensure compatibility with Cisco IOS XR devices running version 24.1.1 and above.

- For devices running Cisco IOS XR version 7.9.21 and earlier, the Layer3-Routing-deprecated sensor paths will remain temporarily supported.

- For devices running Cisco IOS XR version 24.1.1 and above, use the Layer3-Routing KPIs with the new sensor paths designed for seamless integration with newer devices.

Users must select the appropriate sensor paths based on the IOS XR version of their device.

Note When upgrading from an older version of Crosswork Network Controller to 7.1, any KPI profiles containing these KPIs will be disabled during migration. To apply the new sensor paths, users must manually re-enable the KPI profiles after the upgrade.

Table 1: Health Insights KPIs

KPI Name	Description	Alerting	Protocol
Basics			
Device uptime	Monitors device uptime.	Low Single Threshold	MDT, gNMI
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 utilization	Monitors CPU usage across route policies and line cards on routers. Generates an alert when CPU utilization is unusual.	Standard Deviation	MDT, gNMI
Dataplane-Counters			
CEF drops	Monitors CEF drop counters and baseline. Generates an alert for an unusual number of drops.	Rate Change	MDT, 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
IPSLA			
IP SLA UDP echo RTT	Monitors IP SLA UDP echo RTT. Generates an alert when unusual RTT values occur.	Standard Deviation	MDT, gNMI

KPI Name	Description	Alerting	Protocol
IP SLA UDP jitter monitoring	Monitors IP SLA UDP jitter. Generates an alert when an abnormal UDP jitter occurs.	Standard Deviation	MDT, gNMI
LLDP			
LLDP neighbors	Monitors LLDP neighbors.	No Alert	MDT, gNMI
Layer 1-Optics			
Layer 1 optical alarms	Monitors per-port optical alarms (current and past).	No Alert	MDT, gNMI
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 optical FEC errors	Monitors per-port optical FEC errors. Generates an alert when FEC errors exceed the configured threshold.	Rate Change	MDT, gNMI
Layer 1 optical power	Monitors per-port optical power.	No Alert	MDT, gNMI
Layer 1 optical temperature	Monitors per-port optical temperature.	No Alert	MDT, gNMI
Layer 1 optical voltage	Monitors per-port optical voltage.	No Alert	MDT, gNMI
Layer 1-Traffic			
Ethernet port error counters	Monitors port transmit and receive error counters.	Rate Change	MDT, gNMI
Ethernet port packet size distribution	Monitors port transmit and receive packet size distributions.	No Alert	MDT, gNMI
Ethernet port packet statistics	Monitors port transmit and receive packet statistics.	Standard Deviation of Rate Change	MDT, gNMI
Layer2-Interface			
Interface flap detection	Monitors interface flaps and alerts when flap count reaches set threshold.	Two-Level Threshold	MDT, gNMI
Line state	Monitors interface line states.	No Alert	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
Interface packet error counters	Monitors interface transmit and receive error counters. Generates an alert when unusual error rates occur.	Rate Change	MDT, gNMI

KPI Name	Description	Alerting	Protocol
Interface packet error counters (Openconfig)	Monitors interface error counters; generates an alert when unusual error rates occur. This KPI uses openconfig-interfaces YANG model. **Note** In Crosswork Network Controller version 7.1, the sensor paths for this KPI have changed. When upgrading from an older version, KPI profiles that include this KPI will be disabled and must be manually re-enabled to apply the new sensor paths.	Rate Change	gNMI
Interface packet counters	Monitors interface transmit and receive counters. Generates an alert when unusual traffic rates occur.	No Alert	MDT, gNMI
Interface rate counters	Monitors interface statistics as rate counters. Generates an alert when unusual traffic rates occur.	Standard Deviation	MDT, gNMI
Interface rate counters (Openconfig)	Monitors interface statistics (such as rate counters), and generates an alert when unusual traffic rates occur. **Note** In Crosswork Network Controller version 7.1, the sensor paths for this KPI have changed. When upgrading from an older version, KPI profiles that include this KPI will be disabled and must be manually re-enabled to apply the new sensor paths.	Rate Change	gNMI
SNMP interface packet error counters	Monitors interface transmit and receive error counters. Generates an alert when unusual error rates occur.	No Alert	SNMP
SNMP interface packet counters	Monitors interface transmit and receive counters.	No Alert	SNMP
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 3-Routing **Note** In Crosswork Network Controller version 7.1, sensor paths for Layer 3-Routing KPIs have changed to support Cisco IOS XR devices running version 24.1.1 and above. When upgrading from an older version, KPI profiles that include these KPIs will be disabled and must be manually re-enabled to apply the new sensor paths.			
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
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

KPI Name	Description	Alerting	Protocol
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
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
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
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
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
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
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
RIBv6 connected route count	Monitors RIBv6 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
RIBv6 local route count	Monitors RIBv6 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
RIBv6 static route count	Monitors RIBv6 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-deprecated

Note
The sensor paths for these KPIs are compatible with Cisco IOS XR devices running version 7.9.21 and earlier.

IPv6 RIB BGP route count deprecated	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
IPv6 RIB IS-IS route count deprecated	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

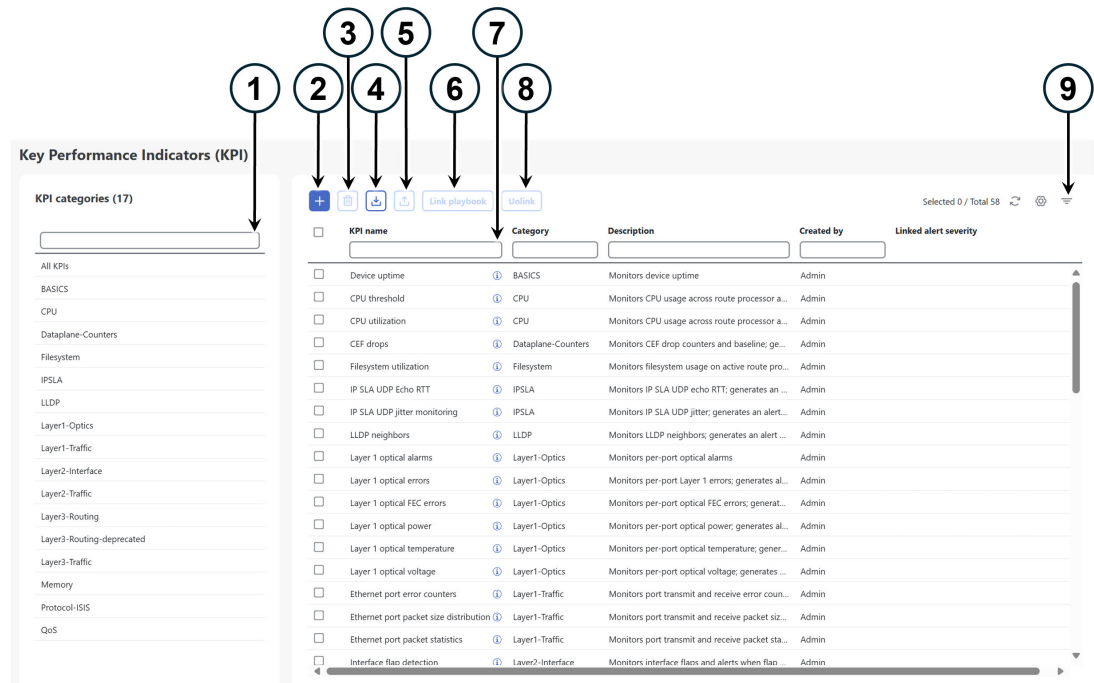| KPI Name	Description	Alerting	Protocol
IPv6 RIB OSPF route count deprecated	Monitors IPv6 RIB for route count and memory used by OSPF. Generates an alert when an anomaly is detected (such as significant increase or decrease in route counts).	Standard Deviation	MDT, gNMI
RIB BGP route count deprecated	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
RIB connected route count deprecated	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
RIB IS-IS route count deprecated	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
RIB local route count deprecated	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
RIB OSPF route count deprecated	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
RIB static route count deprecated	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
RIBv6 connected route count deprecated	Monitors RIBv6 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
RIBv6 local route count deprecated	Monitors RIBv6 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
RIBv6 static route count deprecated	Monitors RIBv6 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-Traffic			
Interface counters by protocol	Monitors interface statistics (such as incoming and outgoing packets or byte counters) organized by protocol.	No Alert	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

KPI Name	Description	Alerting	Protocol
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
Protocol-ISIS			
ISIS neighbor summary	Monitors ISIS neighbor summaries for changes in neighbor status.	No Alert	MDT, gNMI
QoS **Note** In Crosswork Network Controller version 7.1, sensor paths for QoS KPIs have changed. When upgrading from an older version, KPI profiles that include these KPIs will be disabled and must be manually re-enabled to apply the new sensor paths.			
Interface QoS (egress)	Monitors interface QoS on the egress direction for queue statistics, queue depth, and so on.	No Alert	MDT, gNMI
Interface QoS (ingress)	Monitors interface QoS on the ingress direction for queue statistics, queue depth, and so on.	No Alert	MDT, gNMI

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.

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

Figure 1: Key Performance Indicators (KPI)

Item	Description
1	**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.
2	**Add KPIs**: Click ➕ to add a new, user-created KPI. For help with this task, see Create a new KPI, on page 11.
3	**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** You can delete user-created KPIs only. You cannot delete Cisco-supplied KPIs.

Item	Description
4	**Import KPIs**: Click ⬇ to import new user-written or Cisco-supplied KPIs. **Note** When upgrading from an older version of CNC, it's important to consider the following: Before attempting to load a KPI, ensure that it complies with the requirements of the current release. If you try to load a KPI that was created for a previous release and is not compatible, you will receive an error message. 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 appear in the list of KPIs, with each KPI name and category assigned based on the definition in the KPI itself. In order for Health Insights to import them, KPI files must: • 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 on Cisco DevNet.
5	**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.
6	**Link Playbooks**: Select a KPI and then click [Link Playbook] to link it to a playbook. Linking a playbook streamlines the remediation process by importing data from the alert and using it to pre-populate the parameters the playbooks needs (such as device, interface names, and so on) to run in order when you attempt to remediate the issue. For help with this task, see Link KPIs to playbooks and run them manually, on page 13.
7	**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. Filtering is case-sensitive. Click ⊗ to clear any filter criteria you may have set.
8	**Unlink Playbooks**: Select a KPI with a linked playbook and then click [Unlink] to unlink the playbook. You will be prompted to confirm that you want to unlink the playbook. Click **Unlink** to confirm.
9	**Filter**: Click ≡ to set filter criteria on one or more columns in the table.

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 use GNMI as the transport and use sensors that are based on Open Config (OC) YANG modules for collecting telemetry data (with GNMI transport). The requirements for this feature are:

- GRPC must be configured in your device.

- The device properties, while onboarding, must include 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 which is based on 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:

Before you begin

Make sure that the device packages for the devices you want to monitor are available in Crosswork. If they are not available, perform the Add custom packages procedure given in the *Cisco Crosswork Network Controller Administration* guide. Then continue with the steps below.

Procedure

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 seconds between data collections . 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. Only one gather path is supported for user-created KPIs.

Note

If the devices are not listed in the default YANG modules, you can expand the device coverage. Perform the Add custom packages procedure given in the *Cisco Crosswork Network Controller Administration* guide, then continue with the subsequent steps in this procedure.

Click **Next** to display the **Select alert templates** window. You can select from the following alerting types:

- **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.

You can also use the following additional alerting types when you export and modify a prebuilt KPI to create a KPI with custom parameters:

- **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.

Note

To build a KPI that uses data from more than one module, you can do this with KPI profiles and alert groups. For more information, see Create a new KPI profile, on page 18.

Step 6 Choose the alert template that 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 HI Subservice class** 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 HI Subservice class** 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. You 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 vary, as appropriate, for each KPI.

Link KPIs to playbooks and run them manually

The default option for KPI-linked playbooks is for the network operator to run them manually, when an alert is displayed. Crosswork displays the linked playbooks as options, and the operator can select which playbooks to run. However, if Device Override Credentials are enabled properly, you have the option to run one or more KPI-linked playbook automatically, whenever the linked KPI raises an alert, as explained in .

> **Note** You can't use this function if you haven't installed the Change Automation Crosswork application. If that's the case, Crosswork will not display the UI features that link Health Insights KPIs and Change Automation playbooks (for example, you won't see the Link Playbook icon).

You can specify the **Source** of the parameter values the linked playbooks use when you run them. When linking a playbook to a KPI alert, you can select these sources:

- **Playbook**: Use default values coded into the playbook itself

- **KPI Alert**: Use values that are taken from the alert that is raised by the linked KPI.

- **Run-time Input**: Use values that 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 may 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.

- **Run-time 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 2: Example: Specifying parameter value sources for a linked playbook

Procedure

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 8.

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 to see.

Step 5 When you have found the playbook that you want to link to your chosen KPI, click the playbook name. The right side of the window will then list the **Playbook details** for the selected playbook, including:

- The **Hardware platform** and **Software platform** with which the playbook is compatible.

- The minimum software **Version** required to execute the playbook.

- The **KPI alert severity** level needed to trigger a run of this playbook. Note that, if you will be choosing multiple playbooks to run when a KPI alert is raised, be aware that playbooks do not share severity levels. If you have selected a **Critical** severity level for one playbook, you must select **Major**, **Minor**, **Warning** or **Info** severities for a second playbook, and another still for a third playbook.

- Choose the **Set playbook execution** function you want to use. **Manual** execution is the default and is recommended for most purposes. See Link KPIs to playbooks and run them automatically, on page 15 before selecting the **Automatic** execution option.

- Modify the **Set playbook parameters** default values to be used when the playbook runs. In many cases, you can select from a range of default values. You can also enter your own. These values vary widely, depending on the playbook and its purpose. For help, see the information offered on screen for the playbook you have selected.

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 playbooks shown next to the name of the KPI in the **Key Performance Indicators (KPIs)** list.

Step 8 If you want to run more playbooks (up to three playbooks total): Repeat steps 5 through 7 for each additional playbook you want to run when an alert for this KPI is raised.

Step 9 To change the playbook parameters linked to a given KPI, repeat steps 5 through 7 for that KPI, but this time choose the playbook whose settings you want to modify. If you have chosen multiple KPIs, you can switch among them by clicking on the playbook tiles at the top of the window. To unlink a playbook entirely, select the KPI and click Unlink .

Link KPIs to playbooks and run them automatically

In addition to running KPI-linked playbooks only at the network operator's discretion, you can choose to run one or more of your KPI-linked playbooks automatically, whenever the KPI linked to that playbook raises an alert of sufficient severity.

Note You can't use this function if you haven't installed the Change Automation application. If that's the case, Crosswork will not display the UI features that link Health Insights KPIs and Change Automation playbooks (for example, you won't see the Link Playbook icon).

All of the same considerations in setting playbook values described in Link KPIs to playbooks and run them manually, on page 13 apply to this automatic option. Note, however, that:

- You must ensure that none of the required linking parameters are left empty. The user interface indicates the required parameters.

- You must not set any of the form fields as "runtime" parameters. If you are running playbooks automatically, you will not have the option to choose a value at runtime.

- If you are a non-admin user, ensure that you have access to the **Auto Remediation** task. Unless you have access to this task, you cannot unlink or link KPIs to playbook with automatic remediation.

  Prerequisites:

  - Ensure that the Health Insights application is installed.

  - Ensure that **Playbook job scheduling** is enabled and **Credential prompt** is disabled in the Device Override Credentials page. For more information, see Verify installation and configure system settings.

You must have Crosswork system administrator privileges to change these settings. Once these settings are saved, you cannot change them unless you first use the Crosswork Manager to uninstall, then reinstall both the Change Automation and Health Insights applications.

To enable the task permission, do the following:

1. Go to **Administration** > **Users and Roles** > **Roles**.

2. Under the **Roles** pane, select the role for which you want to grant the access.

3. Under the **Task Permissions** tab, enable the **Auto Remediation** check box and click **Save**.

Procedure

Step 1 From the main menu, choose **Performance Alerts** > **Key Performance Indicators (KPI)**. The **Key Performance Indicators (KPI)** window opens, listing the KPI categories and the KPIs available in each category.

Step 2 Select the KPI you want to link to one or more playbooks. You can use filters to find the KPI you want, as explained in Manage KPIs, on page 8.

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 to see.

Step 5 When you have found the playbook that you want to link to your chosen KPI, click the playbook name. The right side of the window will then list the **Playbook details** for the selected playbook, including:

- The **Hardware platform** and **Software platform** with which the playbook is compatible.

- The minimum software **Version** required to execute the playbook.

- The **KPI alert severity** level needed to trigger a run of this playbook. Note that, if you will be choosing multiple playbooks to run when a KPI alert is raised, be aware that playbooks do not share severity levels. If you have selected a **Critical** severity level for one playbook, you must select **Major**, **Minor**, **Warning** or **Info** severities for a second playbook, and another still for a third playbook.

- Under the **Set playbook execution** field, select **Automatic**. Note that, if you or a Crosswork administrator have not already done so, Crosswork will prompt you to enable **Playbook job scheduling** (and disable **Credential prompt** overrides) in order to enable automatic playbook execution.

- Modify the **Set playbook parameters** default values to be used when the playbook runs. In many cases, you can select from a range of default values. You can also enter your own. These values vary widely, depending on the playbook and its purpose. For help, see the information offered on screen for the playbook you have selected.

Step 6 Verify or modify the **Source** and other 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 playbooks shown next to the name of the KPI in the **Key Performance Indicators (KPIs)** list.

Step 8 If you want to run more playbooks (up to three playbooks total): Repeat steps 5 through 7 for each additional playbook you want to run when an alert for this KPI is raised.

Step 9 To change the playbook parameters linked to a given KPI, repeat steps 5 through 7 for that KPI, but this time choose the playbook whose settings you want to modify. If you have chosen multiple KPIs, you can switch among them by clicking on the playbook tiles at the top of the window. To unlink a playbook entirely, select the KPI and click Unlink .
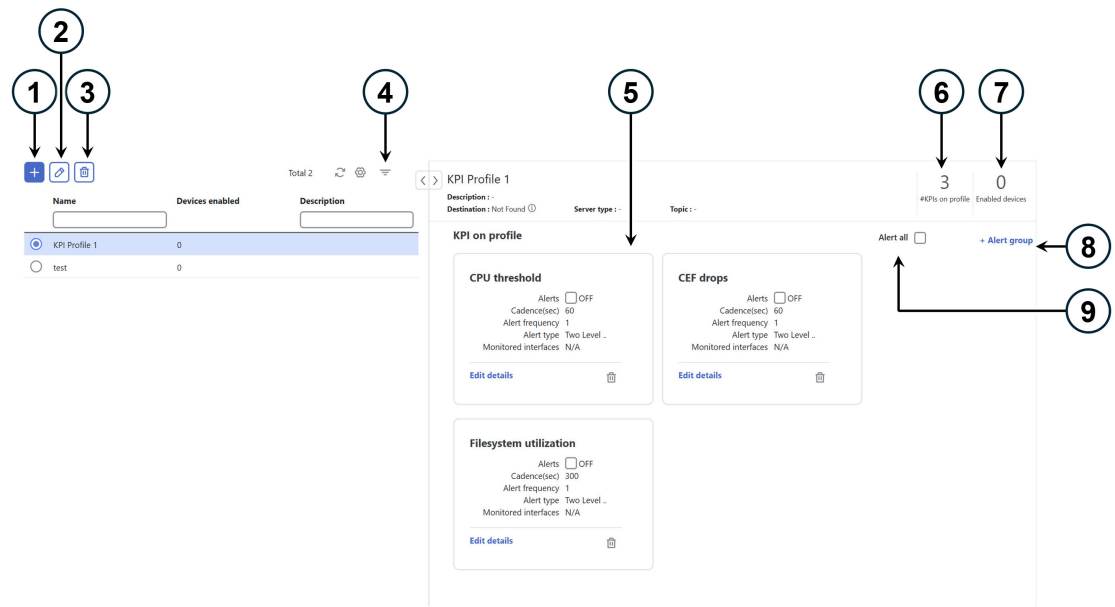
Manage KPI profiles

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 that is 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 the collection jobs on the Crosswork Data Gateway for all the KPIs and for MDT-based KPIs, this removes the configuration in the device(s).

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

Figure 3: KPI profiles

Item	Description
1	**Create KPI profile**: Click ➕ 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 ✏ to edit it.
3	**Delete KPI profile**: Select a user-created KPI profile in the list and then click 🗑 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 ≡ to clear any filters you have set. Filtering is case-sensitive.
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. For KPI profiles with custom KPI, the Alert checkbox will be disabled, and an alarm will be raised to inform users that alerting is disabled for the profile.

Item	Description
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
9	**Alert All**: Click this option to turn off or turn on the alerts for all KPIs in the profile.

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 these tasks.

Procedure

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.

To avoid problems with alerting, ensure that each KPI **Profile name** you assign is unique and does not share sub strings with other KPI profiles. For example: In a set of three KPI profiles with the IDs "L2", "L2SNMP" and "L2GRPC", all three profiles IDs contain the sub string "L2".

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 Add or edit a data destination in the *Cisco Crosswork Network Controller Administration* guide.

Step 5 Add KPI to the profile, using the following filter options:

    a) **All KPIs**: By default, this option is selected and all available KPIs are displayed in the list. You can select the desired KPI by checking the relevant check box.

    b) **Recommended KPIs**: Use this option if you want the system to recommend KPIs for your devices. Clicking **Recommended KPIs** displays a list of your devices from the network. You can filter the device list by entering relevant values in the Name field, or by using tags. Select a device from the list to show recommended KPIs on the right side. Select the desired KPI by checking the relevant check box.

> **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 profiles 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.

> **Note**
>
> For the Interface KPIs, you can gather the data for **all** the interfaces or **selected** interfaces. If you opt to gather the information for **all** the interfaces, a warning symbol appears on the KPI profile name on the left side and on the individual KPI details on the right side, indicating that the monitoring interfaces are not customized.

> **Important**
>
> Gathering telemetry data for all the interfaces can be resource-intensive and may require additional worker nodes and/or CDG resources to be deployed.

Step 8   You can leave the KPI parameters at the default or choose a different value. To edit the KPI parameters and preferences, click **Edit details**, and the **KPI details** window is displayed. Edit the values as appropriate for the purpose of your KPI. The details are:

- **Common parameters**

  - **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 group 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".

- **KPI monitoring preferences**: Applicable only for Interface KPIs.

Figure 4: KPI monitoring preferences

- **Customer selected interfaces**: You can define the interface criteria.

    - **Regex**: You can define a rule using regex expression.

    - **Add manual query**: You can add different sets of rules.

- **All interfaces**: The selected KPI is applied to all the interfaces.

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 profiles on devices, on page 21.

See Disable KPI profiles on devices or device groups, on page 24 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 group logic query. To create an alert group, click + **Alert group**. The **Create alert group** window is displayed.

Note

Configuring an alert provider enables the alerts from the group alert to be sent to a REST endpoint using Webhook registered in the alert provider.

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.

Figure 5: Create alert group

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 profiles 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 network devices operate most efficiently when configured to only report data that specifically relates to the performance of its role in the network.

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.

• Do not enable KPI profiles on devices that are not reachable.

• The load that is created on Data Gateway and Platform Infrastructure caused by enabling KPI profiles on many devices or KPI profiles that gather a lot of data is hard to estimate. Crosswork provides a UI and API that allows you to see the current load and provides general guidelines for determining when you must refrain from enabling more collections until either other collections are disabled or more resources (Data Gateway or worker nodes) are added. To check Data Gateway load, see Crosswork Data Gateway health metrics in the *Cisco Crosswork Network Controller Administration* guide.

To enable KPI profiles on devices:

Procedure

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.

Figure 6: Devices window

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 that 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 that you want. The names of all the devices in that group appear in the devices table on the right.

Note

You cannot enable a KPI on a device that is attached to a standard Crosswork Data Gateway. Also, you cannot move a KPI-enabled device from extended Crosswork Data Gateway to standard Crosswork Data Gateway. In both cases, Crosswork displays an error pop-up.

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 that 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 pop-up window provides the details of the KPI. Click the ✕ to close the pop-up 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.

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.

Enabling a KPI results in configuring a collection job on the Crosswork Data Gateway. For GNMI-based and SNMP-based KPIs, the Crosswork Data Gateway polls the desired data and forwards it to Health Insights for processing and evaluation. For MDT-based KPIs, the devices (through NSO) are configured to push the data to the Crosswork Data Gateway which then forwards it to Health Insights for processing and evaluation.

In the **Device** table, in the **Enabled profiles** column, you can click the number to see the status of the KPI collection job (for example to see if the KPI profile ID is active or not).

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 the job sets complete with a "Partial" or "Failed" status, ensure to read the job completion messages, and check that the selected devices are still reachable.

Figure 7: KPI Job History

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 **Administration** > **Collection Jobs** to look at the collection jobs and to make sure that they are created and the incoming data is collected. For more information on monitoring the status of collection job, see the Monitor collection jobs section in the *Cisco Crosswork Network Controller Administration* guide.

Step 9 From the main menu, choose **Performance Alerts** > **Alert Dashboard**. The Health Insights alert dashboard, on page 25 shows the alert status for the devices on which you have enabled KPI monitoring.

- 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 profiles per device takes around 3-5 seconds (but the time varies based on the number of KPIs being enabled). If the device is not reachable, it keeps trying until it is timed out. This may result in the job taking more time to reach the completed state.

Verify the deployment status of enabled KPIs

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

Procedure

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.

Any KPI job stuck in the processing state that does not complete within 60 minutes will be marked as "failed". After addressing any underlying issues (for example, device connectivity, credentials, NSO sync, and so on), the same job must be reactivated, as explained in Create a new KPI, on page 11.

Disable KPI profiles 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.

Procedure

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 check box 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) used on the devices from which you no longer want to collect the KPI data.

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.
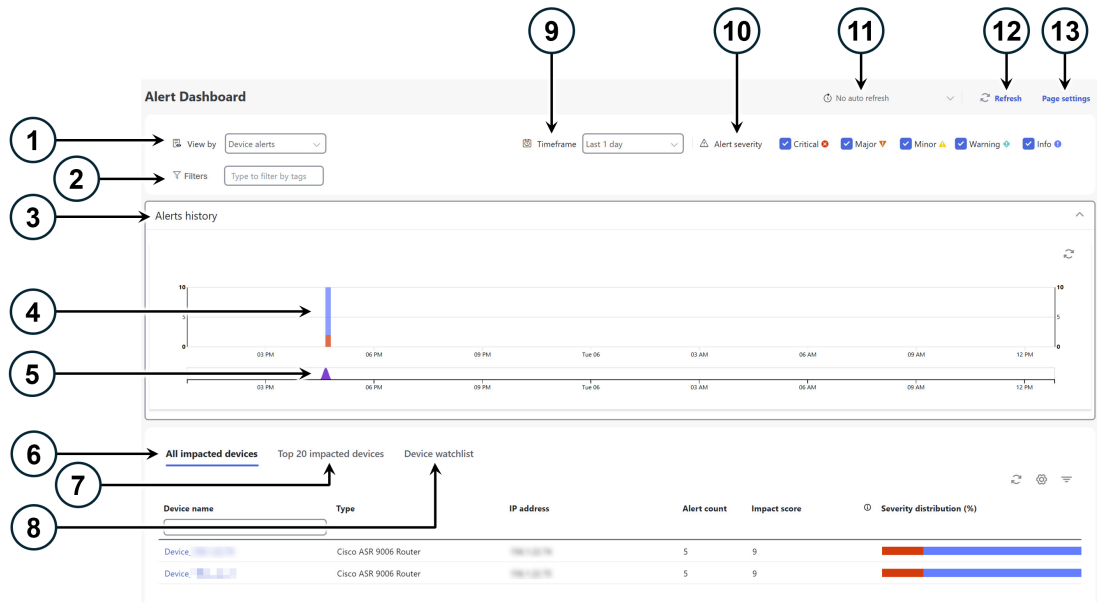
Health Insights alert dashboard

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, although 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.

Figure 8: Health Insights Alert Dashboard

Item	Description
1	**Device/KPI Alert selector**: Click here to toggle between device alert and KPI alert information.
2	**Filters**: This field lets you filter the alert dashboard information by associated tag names. To select a tag, do one of the following: • 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: 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 that you want to use and then click **Apply filters**. 4. Delete the character that you typed in Step 1 to clear the results list. Tag filters you create are not saved. If you open another window and then return to the alert dashboard, you need to re-create tag filters.
3	**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.
4	**Alerts history bar graph**: This graph 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.

Item	Description
5	**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: **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. 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**.
6	**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: • 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: (5 x number of critical alerts) + (4 x number of major alerts) + (3 x number of minor alerts) + (2 x number of warning alerts) + (1 x number of info). These are the default values. You can change the weightage in the **Page settings** option. 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	**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. Also, the tiles are color coded. The colors correspond to the **Alert severity**. To view more detailed information for a particular device or KPI, click the device or KPI name link in the center of the tile.

Item	Description
8	**Device/KPI watchlist**: When selected, this dashlet provides a list of all devices or KPIs, that you had selected from + **Manage device/KPI watchlist**, which are affected by alerts. The information for each affected device or KPI includes: • 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.
9	**Timeframe**: Specifies the time period for which the dashboard provides alert information: The last one hour, last day, last three days, last week, and last month. Please note that the dashboard provides alert information only, not telemetry information.
10	**Alert severity**: 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 check box for that severity. An enabled check box indicates that alerts of that severity have been raised and are being displayed. A clear check box indicates that the alerts of that severity are either not being displayed or have not been raised during the displayed time period.
11	**Auto refresh**: Specifies how often the dashboard is automatically refreshed.
12	**Refresh icon**: Refreshes the dashboard.
13	**Page settings**: Provides the default page settings for that particular session. You can customize the page display based on Alert type, Timeframe, Auto refresh, Detail display, and Alert severity. You can also change the weightage here for the impact score calculation.

Note The individual alerts for any specific KPI are shown in the dashboard. Alerts resulting from the alert group logic are not shown in the dashboard. Only the API shows the impacted results.

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.
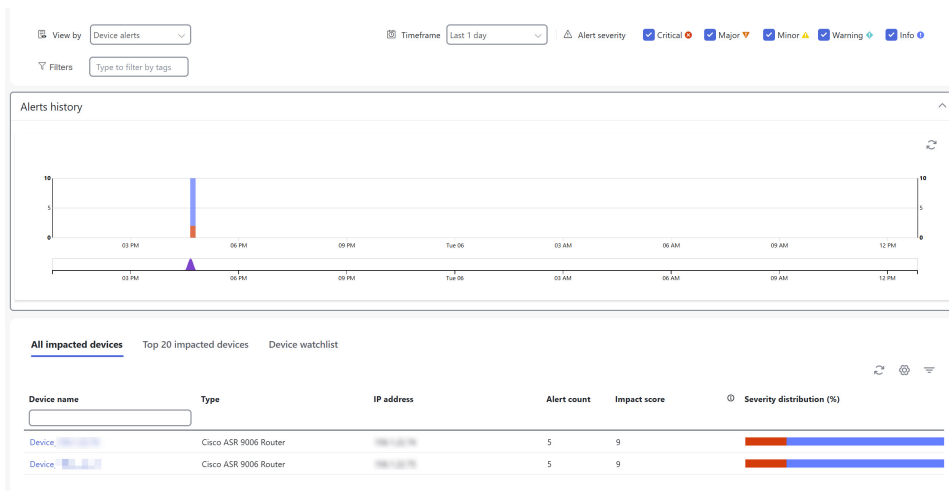
| **Note** | The KPIs shown in the following steps are examples. There are many more KPIs available in Health Insights. For the complete list, see List of Health Insights KPIs, on page 2. |

Procedure

Step 1 From the main menu, choose **Performance Alerts** > **Alert Dashboard**. The Health Insights Alert dashboard is displayed.
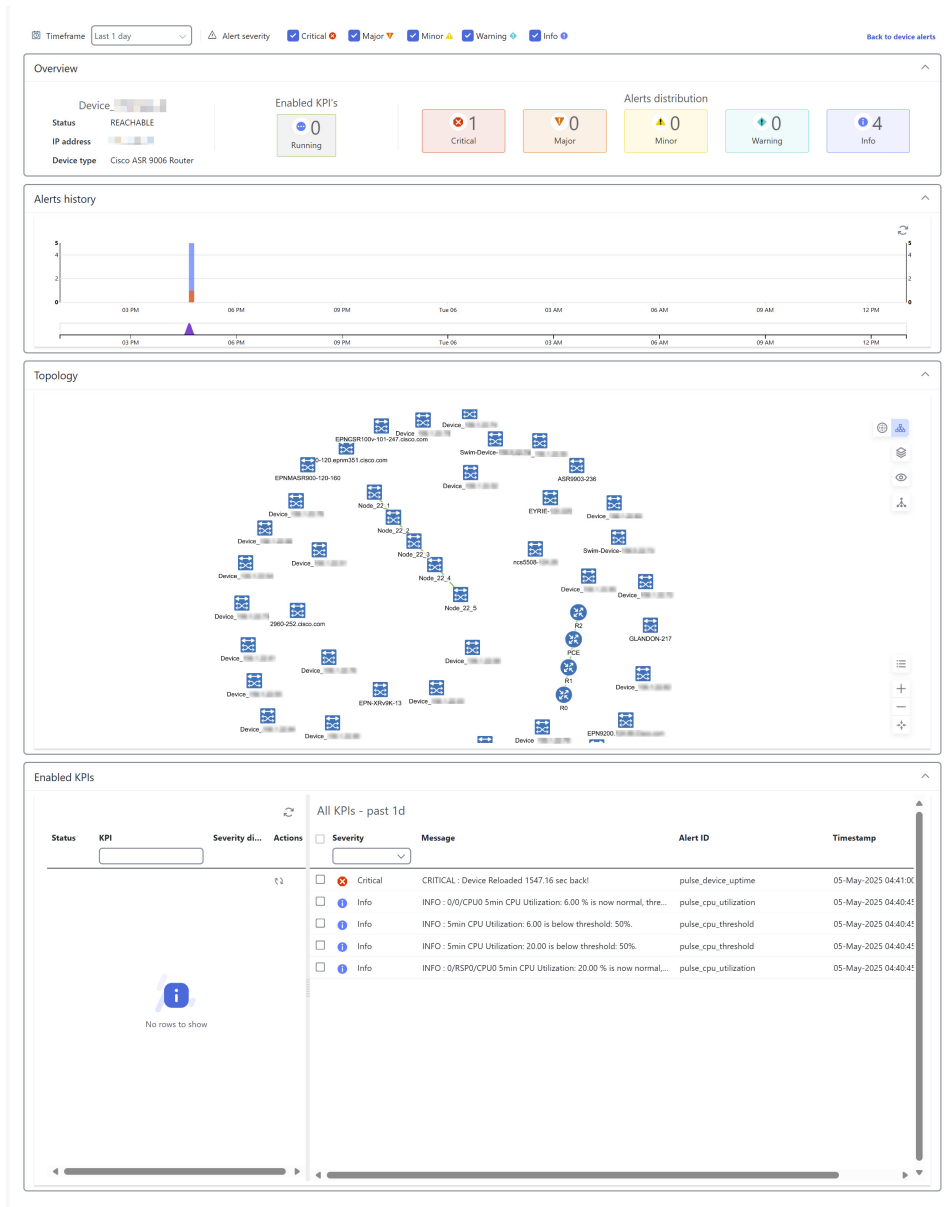
Figure 9: Alert Dashboard

Step 2 Make sure that the **Device alerts** view is displayed (select the **View by: Device alerts** toggle, if needed). Then scroll down below the **Alert history** panel and click the **All impacted devices** tab. The dashboard displays a list of devices with alerts.
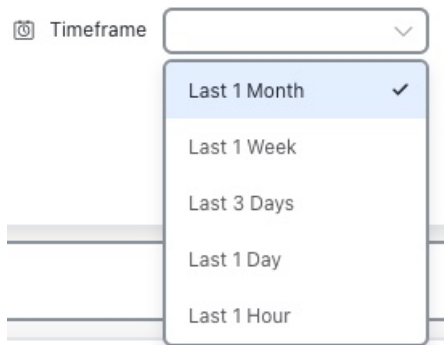
Step 3 Click the **Device name** for the device whose details that you want to view. Health Insights displays the device's basic **Overview** information, **Alert history**, a **Topology** map, and the list of the device's currently **Enabled KPIs**.

Figure 10: Device alert details

The **Topology** map is a version of the map that you see when you select **Topology** from the main menu, but centered on the device for which you are viewing KPI alerts. The **Enabled KPIs** panel lists all the KPIs currently enabled on the selected device, plus a list of all the alerts for that device raised by any of the enabled KPIs during the past hour.

To see alerts for a different period, click the **Timeframe** dropdown (shown below) and select the time frame you want (up to `Last 1 Month`).

Figure 11: Timeframe dropdown

To focus the display only on alerts of the severity you want, check or uncheck the boxes in the **Alert severity** field, (shown below).

Figure 12: Alert severity

Step 4   To view telemetry data received for any of the KPIs for this device: In the **Enabled KPIs** list on the left, click the icon next to the KPI whose telemetry data you want to see. Crosswork displays a popup telemetry data window like the one shown below. The popup window shows a timeline at the top, representing all the alert data received during the last 72 hours (with hourly slots), and relevant performance for the same period in a Grafana graph at the bottom.

Step 5   The timeline shows a blue box, with brushes on the sides, representing the limits of the time period shown in the graph at the bottom. Click on and move the blue box or the brushes on the timeline to select the desired time slot (up to 6 hours). Move the mouse cursor over any data point in the graph to view additional pop-up information for that data point.

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.

Graphical data is only visible for time slots for which alerts were triggered. Be default, the Grafana graph shows telemetry for the last six hours.

Step 6   To focus the Grafana view on a different timeframe, click the time period field (with the clock icon) shown at the top of the **Summary** tab. You can select time periods up to several years.

Telemetry data retention in the Alerts dashboard

Telemetry data collected from devices is retained in the time-series database for the last 72 hours. This data 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 database and are retained for 30 days. The messages showing the alerts' duration are displayed at the top of the Device/KPI view in the Alert dashboard. For more information, see View alerts for network devices, on page 28. The alerts can also be queried using REST APIs. For more information, see the Cisco Crosswork Network Controller API Documentation on Cisco DevNet.

Troubleshoot Health Insights

The following table describes issues that 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.	1. Go to **Performance Alerts** > **KPI Job History** and check the **Message** column for an error message. 2. Go to **Device Management** > **Network Devices**. 3. For the failed device, in the **NSO state** column, click ⓘ. 4. From the **Check sync** drop-down list, click **Sync from**. 5. Confirm that the device is in sync now.
Operation timeouts can occur when adding a new KPI to an existing KPI Profile and then editing the newly added KPI.	Write times for KPI edits can take up to five minutes, so the edited KPI in the profile will be enabled eventually. If you find the timeout message a problem, you may want to disable the KPI profile for a short period until the write delay has passed.
Health Insights not receiving data.	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**. 3. Check for the collection job to see if the table (accessed by clicking the graph icon for the job) indicates that data collections are processing.