Monitor Devices

View Device Status

You can view device status to view connectivity and any errors.

Step 1 In the main window, click **Monitor** > **Devices**.

A list of previously added devices is displayed.

Step 2 Click on a device name in the **Device** column.

Detailed device information is displayed. By default, the **Status** tab is selected and displays overview information about the device. (Depending on the applications for which you have a license, separate product tabs also appear.)

Step 3 On the **Status** page, verify that there are no connectivity errors. Green arrows indicate working connectivity.

a. Verify the connection between Applications and Crosswork Data Gateway is working.

b. Verify the connection between Crosswork Data Gateway and the devices.

Step 4 Hover your cursor over any fields to display more details.

Step 5 To export a .json file containing device status, click **Export Status Report**.

View Device Traffic Details

You can view the receive (RX) and transmit (TX) traffic information for the devices that you added.

Note The data displayed in the graph may be delayed by five minutes since Netflow data is sent to the system every five minutes.

Step 1 In the main window, click **Traffic Analysis** > **Monitor** > **Devices**.

A list of previously added devices appears.

Step 2 Click the name of the device for which you want to see the details. By default, the Traffic Analysis tab is displayed.

Step 3 By default, the **Graphs** tab opens and displays RX and TX traffic metrics. From the Time drop-down list, select the timeframe for which you want to view the traffic information.

Step 4 After you make any changes, click the **Refresh** icon to update data.

Step 5 To view traffic details for the device interfaces, click the **Interfaces** tab.

Step 6 To view specific RX and TX data for an interface, click the interface name.

Step 7 To designate an interface as internal or external, check the check box next to one or more interfaces, then choose **Set External** or **Set Internal**.

The **Type** column updates to display the interface type.

View Trust Insights Details

You can view Crosswork Cloud Trust Insights details for devices you previously added.

Step 1 In the main window, click **Trust Insights** > **Monitor** > **Devices**.

A list of previously added devices appears.

Step 2 Click on the name of the device for which you want to see the details.

Step 3 By default, the **Trust Insights** tab opens. The rest of the device details page contains information organized into separate tabs. The following table describes the device detail information displayed under each tab.

Table 1: Trust Insights Device Detail Descriptions

Tab	Description
Platform	Displays information similar to the output of the *show platform* CLI command. To view more details, click the following tabs: • **Hardware**—Lists hardware node, type, state, HA state, and last seen information. Click on a name in the Node column to display specific information about that node. Crosswork Cloud Trust Insights displays a history of where this individual component was previously observed. The hardware component history tracks individual hardware FRUs, based on their confirmed serial number, across systems over time. • **Package Insights**—Lists packages on the device that are deactivated or have not been committed. The state can be one of the following: • **Active - Uncommitted**—The package is actively running on the device. If you want to save these changes, commit the package prior to rebooting the device. • **Deactivated**—The package is not actively running on the device. You can commit this change, otherwise the package will be active again after the device reboots or is activated manually. • **Packages**—Lists all the software packages. For more information, see View Device Software Changes, on page 4. • **Mismatched Files**—Displays a list of mismatched files on this device. For more information, see View Device Package Mismatched Files, on page 6.
Inventory	Lists the device hardware details such as serial numbers, models, firmware, and other information.
Changes	Shows hardware and software changes made to the device. See View Device Changes, on page 4 for more information.

View Device Inventory

Crosswork Cloud Trust Insights can display details about your hardware inventory, which can be helpful if you are troubleshooting hardware issues.

Step 1 In the Crosswork Cloud Trust Insights main window, click **Trust Insights > Monitor > Devices**.

Crosswork Cloud Trust Insights displays a list of previously added devices. See Add Devices for more information.

Step 2 Click on the name of the device for which you want to see inventory details.

If **Connected** appears next to the device name, the Crosswork Data Gateway has successfully connected to the device.

Step 3 Click the **Inventory** tab.

Crosswork Cloud Trust Insights displays all the hardware associated with the device you selected.

View Device Changes

You can view the device changes to understand what and when hardware and software changes were made.

Step 1 In the main window, click **Trust Insights > Monitor > Devices**.

Crosswork Cloud Trust Insights displays a list of devices that were previously added. See Add Devices for more information.

Step 2 Click on the name of the device for which you want to view the changes.

Crosswork Cloud Trust Insights displays overview information about the device.

Step 3 Click the **Changes** tab.

Trust Insights highlights observed events over a historical timeline for the device you selected.

Step 4 Click on a time frame for which you want to see the device changes.

Step 5 Click **Hardware** to view the hardware change details for the timeframe you selected.

Step 6 Click **Software** to view the software change details for the timeframe you selected.

Step 7 Click **Changes Only** to display only values that changed from the start to the end of the time period you selected.

View Device Software Changes

Crosswork Cloud Trust Insights provides a way to understand what software changes were made on your devices. You can view specific software changes made to your devices and observe where there are software mismatches between Known Good Values (KGVs) and what your device is currently running.

Step 1 In the main window, click **Trust Insights > Monitor > Devices**.

Crosswork Cloud Trust Insights displays a list of devices that were previously added. To add devices, see Add Devices for more information.

Step 2 Click on the name of the device for which you want to view the changes.

Step 3 By default, the **Trust Insights** tab opens.

Step 4 Under the **Platform** tab, click **Packages**, which appears under the graph.

Crosswork Cloud Trust Insights lists all the software packages.

In the **Package Integrity** column, Crosswork Cloud Trust Insights displays one of the following values:

- Changes detected—Indicates the correct software package was installed, but changes were made after the installation.
- Mismatch—Indicates the installed software package does not match the Known Good Value (KGV).
- Mismatch and changes detected—Indicates the installed software package does not match the KGV and changes were made after the installation.
- OK—The installed software package matches the KGV.
- Not supported—The software package fingerprint is missing in the dossier. You need to install an SMU that supports package integrity measurements, if available for the device.

  Note Cisco IOS XR Release 7.3.1 and later releases supports the fingerprint of packages. This feature helps in verifying the authenticity of an installable package using a Known Good Value (KGV) for each package. The installed and running software is compared with the KGV to determine whether the package is genuine.

- No KGV data—Crosswork Cloud Trust Insights is unable to compare the software package with KGVs because the package fingerprint is missing in the KGV. Crosswork Cloud Trust Insights does not recognize the package.

Step 5 Click on a link in the **Package Integrity** column to view additional details about the software files and packages on your device.

Crosswork Cloud Trust Insights displays the Software Integrity Analysis, which includes the following details:

- Package Signature Analysis—Displays details about any changes detected in the package signature. Crosswork Cloud Trust Insights evaluates the installed packages and displays measurements to indicate if the package signature is trustworthy. The following fields indicate package signature changes, and you can quickly validate if any of the hashes do not match:
  - Known Good Values Hash—Value designated by Cisco or previously designated in Crosswork Cloud Trust Insights.
  - Package Install Hash—Value at the time the package was installed.
  - Package Runtime Hash—Value of the package during runtime.
- File Signature Analysis—Displays details about the changes detected in the file signature. Each file that contains a mismatch is displayed along with the details about the mismatch. If a file does not have any mismatches, it does not appear in the list. You can view the hashes displayed in the columns to view where the mismatches occur. To quickly

view a list of mismatched files on this device click the **Mismatched Files** tab (see View Device Package Mismatched Files, on page 6).

View Device Package Mismatched Files

Crosswork Cloud Trust Insights allows you to quickly view a list of mismatched package files for a particular device. Mismatched files indicate software mismatches between Known Good Values (KGVs) and what your device is currently running.

Step 1 In the main window, click **Trust Insights > Monitor > Devices**.

Crosswork Cloud Trust Insights displays a list of devices that were previously added. To add devices, see Add Devices for more information.

Step 2 Click on the name of the device for which you want to view the mismatched files.

Step 3 By default, the **Trust Insights** tab opens.

Step 4 Under the **Platform** tab, click **Mismatched Files**, which appears under the graph.

Crosswork Cloud Trust Insights lists all the mismatched files found on that device.

In the **Mismatch Status** column, Crosswork Cloud Trust Insights displays one of the following values:

- **Runtime**—The KGV value does not match the value of the file during runtime.
- **OnDisk**—The KGV value does not match the hash of the file content currently on the disk.
- **OnDisk & Runtime**—The KGV value does not match the value of the file during runtime and the value at the time the package was installed.
- **Unknown**—Crosswork Cloud Trust Insights cannot determine the KGV value.

Step 5 From the **Mismatch Status** column, click the status value.

a) Click the **History** tab to view the file details. You can view the hashes displayed in the columns to quickly view where the mismatch occurs.

b) Click the **Seen Elsewhere** tab to view a list of devices that also have this mismatched file.

View File Anomalies

Note Devices running the following Cisco IOS XR versions are supported:

- 7.4.1
- 7.4.2
- 7.5.2

To help monitor malicious activity or tampering of Cisco IOS XR devices, you can view a list of unknown files for a particular device. Generally, any files that are "not expected" or significantly deviate from typical IOS XR files are flagged as unknown files. For example:

- Files that do not match known KGV filenames.
- Files where the metadata has changed, yet the SHAsum remains the same.
- Files that have known hashes but the filename or path does not match the KGV.

Step 1 In the main window, click **Trust Insights** > **Monitor** > **Devices**.

Crosswork Cloud Trust Insights displays a list of devices that were previously added. To add devices, see Add Devices for more information.

Step 2 Click on the name of the device for which you want to view unknown files.

Step 3 By default, the **Trust Insights** tab opens.

Step 4 Under the **Platform** tab, click **Unknown Files**, which appears under the graph.

Crosswork Cloud Trust Insights lists details of all the unknown files found on that device.