Cisco Crosswork Data Gateway

This section contains the following topics:

Overview of Cisco Crosswork Data Gateway

Cisco Crosswork Data Gateway is a secure, common collection platform for gathering network data from multivendor devices. It is an on-premise application deployed close to network devices and supports multiple data collection protocols including MDT, SNMP, CLI, gNMI, and Syslog.

The NETCONF data collection support is deprecated starting from the CNC 5.0 release.

The number of Crosswork Data Gateways you need depends on the number of devices supported, the amount of data being processed, the frequency at which it is collected, and the network architecture.

When Crosswork Data Gateway is deployed with Cisco Crosswork Infrastructure (also referred to as Cisco Crosswork in this guide), Cisco Crosswork acts as the controller application.

Crosswork Data Gateway uses the following concepts:

- **Crosswork Data Gateway Instance**: Crosswork Data Gateway instance that you install.

- **Crosswork Data Gateway Profile**: Crosswork Data Gateway supports the following deployment profiles:

  - **Standard**: for use with all Crosswork applications, except Crosswork Health Insights, and Crosswork Service Health (Automated Assurance).

  - **Extended**: for use with Crosswork Health Insights and Crosswork Service Health (Automated Assurance).

> ⚠️
>
> **Attention**   The **Standard with Extra Resources** profile is available as a limited-availability feature and must not be used while deploying Crosswork Data Gateway in your data center. Please contact the Cisco Customer Experience team for assistance.

- **Crosswork Data Gateway Pool**: A logical unit of one or more Crosswork Data Gateway instances with an option to enable high availability. When a Crosswork Data Gateway instance goes down, Cisco Crosswork automatically replaces the instance with a spare instance from the pool to ensure that devices are managed, and data collections have minimal disruption.

- **Crosswork Data Gateway**: A Crosswork Data Gateway instance that is assigned a virtual IP address when it is added to a Crosswork Data Gateway pool.

  Operations such as attaching or detaching devices, creating collection jobs happen on the Crosswork Data Gateway.

- **Data Destination**: Internal or external recipients of data collected by the Crosswork Data Gateway. By default, Cisco Crosswork is defined as a data destination. Other destinations (external users) can be defined using the Cisco Crosswork UI or APIs.

- **Collection Job**: A task that Crosswork Data Gateway has to complete to collect data. Crosswork applications create collection jobs to check device reachability, collect telemetry data needed to determine network and service health. The Cisco Crosswork UI and API allow you to configure collection jobs for non-Crosswork applications.

- **Custom Software Packages**: Files and device model definitions to extend device coverage and support data collection from currently unsupported devices.

> ✎
>
> **Note**   This chapter explains only the Cisco Crosswork Data Gateway features that can be accessed via Cisco Crosswork UI.
>
> For more information about the Interactive Console of Cisco Crosswork Data Gateway instance and how to manage it, see **Appendix A**: Configure Crosswork Data Gateway Instance.

Crosswork Data Gateway UI Overview

To open the Cisco Crosswork Data Gateway management view, log in to Cisco Crosswork and choose **Administration** > **Data Gateway Management** from the left navigation bar.

Figure 1: Data Gateway Management Window
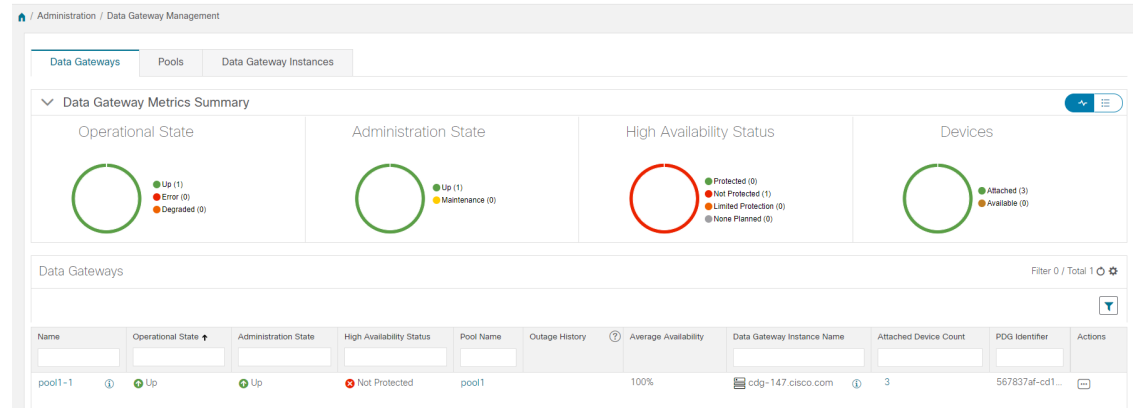
The **Data Gateway Management** page has three tabs:

- **Data Gateways**: Displays details of the virtual Cisco Crosswork Data Gateways in the network. You can attach or detach devices to the Data Gateway from this tab.

- **Pools**: Manages Cisco Crosswork Data Gateway pools.

- **Data Gateways Instances**: Manages physical Cisco Crosswork Data Gateway instances.

You can filter the tables by clicking the legends next to the donut chart visualization. For example, to view the pools with the administration state as **Up**, click the **Up** icon next to the **Administration State** chart. The table filters the pools with the state **Up**.

To select the columns that must be displayed in the table, click the Settings icon in the top-right corner of the table and select the relevant check boxes. In order to hide the columns, clear the check boxes.

All the tables in the Crosswork Data Gateway UI, allows you to multiselect the items by clicking the empty field and choosing **Select all** from the menu. All the selected items are displayed in the table. To clear the selection, click the **X** icon next to the selected item.

The following table explains the various columns in the **Data Gateway Management** page.

Table 1: Cisco Crosswork Data Gateway UI

| Column	Description
Operational State	Operational state of the Cisco Crosswork Data Gateway instance. A Crosswork Data Gateway instance has following operational states: • **Degraded**: The Cisco Crosswork Data Gateway instance is reachable but one or more of its components are in a state other than OK. • **Up**: The Cisco Crosswork Data Gateway instance is operational and all individual components are "OK". • **Error**: The Cisco Crosswork Data Gateway instance is unreachable or some of its components are in Error state.
Administration State	Administration state of the Cisco Crosswork Data Gateway instance. • **Up**: The instance is administratively up. • **Maintenance**: Operations between Cisco Crosswork and the Cisco Crosswork Data Gateway are suspended to perform upgrades or other maintenance activities (for example, uploading certificates).
High Availability Status	High availability status of a Crosswork Data Gateway could be either: • **Protected**: All instances are UP and there is at least one standby available in the pool. • **Not Protected**: All standby instances are DOWN. • **Limited Protection**: Some standby instances are DOWN, but there is still at least one standby that is UP. • **None Planned**: No standby instances were added to the pool during pool creation.
Devices	Number of devices attached to the Cisco Crosswork Data Gateway pool.

Column	Description
Name	Name of the Cisco Crosswork Data Gateway instance. Clicking the ⓘ icon next to the name displays the enrollment details of each instance. This includes details such as, the: • Virtual IP Addresses • Data Gateway Instance Name • Description • Data Gateway Instance Type that indicates the profile of the Crosswork Data Gateway. • Data Gateway Instance UUID Click the instance name to open the Crosswork Data Gateway vitals page. The page displays the operations and health summary of a Crosswork Data Gateway.
Pool Name	Name of the Crosswork Data Gateway pool. On clicking the pool name, the Crosswork Data Gateway vitals page opens.
Outage History	Outage history of the Cisco Crosswork Data Gateway instance over a period of 14 days. State aggregation for a day is done in the order of precedence as Error, Degraded, Up, Unknown and Not Ready. For example, if the Crosswork Data Gateway instance went Unknown to Degraded to Up, color is displayed as Degraded (orange) for that day as Degraded takes precedence over Up and Unknown. If the Crosswork Data Gateway was in Error state at any time during that day, the tile is Red. If the Data Gateway was not in Error but in Degraded State anytime of the day, the tile is Orange. If the DG was not in Error or Degraded state and was only Up, then the tile is Green.
Average Availability	Value indicating the health of the Cisco Crosswork Data Gateway instance. This percentage is calculated as the total time (in milliseconds) a Crosswork Data Gateway was in UP state over the time between start time of first event and end time of last event. **Note** The end time of last event is the current time stamp, so the duration of last event is between its start time and current time stamp.

Column	Description
Data Gateway Instance Name	Name of the Cisco Crosswork Data Gateway that is created automatically when you add a Crosswork Data Gateway instance to a pool. Clicking the ⓘ icon next to the instance name displays the enrollment details of each instance. This includes details such as, the: • Data Gateway Instance Name • Description • Data Gateway Instance Type • Data Gateway Instance Role • CPU • Memory • Number of NICs • Data Gateway Instance UUID • Version • Data Gateway Instance OS • Interface Name • Interface Role(s) • Interface Mac • Interface Name The **Additional Interface Role Information** describes the interface roles available in Crosswork Data Gateway.
Attached Device Count	Indicates the number of the devices that are attached to the Crosswork Data Gateway pool.
PDG Identifier	Unique identifier of the Cisco Crosswork Data Gateway instance.
Actions	Click ⋯ to view the actions that you can perform on the pool: • Attach Devices. For more information, see Attach Devices to a Crosswork Data Gateway, on page 14. • Detach Devices. For more information, see Manage Cisco Crosswork Data Gateway Device Assignments, on page 20. • Move Devices. For more information, see Manage Cisco Crosswork Data Gateway Device Assignments, on page 20. • Initiate Failover. For more information, see Perform a Manual Failover, on page 13.

You can configure the Crosswork Data Gateway dashlet in the **Crosswork Home** page **> Dashboard**. The dashboard allows you to customize the dashlet to display the summary of the Crosswork Data Gateway instances and pools. For information on using Dashboard, see Get a Quick View in the Dashboard.

Set Up Crosswork Data Gateway to Collect Data

Crosswork Data Gateway requires you to complete the following setup tasks first, before it can run collection jobs.

Note　This workflow assumes that you have already installed Cisco Crosswork Data Gateway as explained in *Cisco Crosswork Network Controller 5.0 Installation Guide*.

It is sufficient to complete Step 1 to Step 3 in the following table to get Crosswork Data Gateway set up and running with Cisco Crosswork and other Crosswork applications. Step 4 to Step 6 are optional and required only in case you wish to extend the Crosswork Data Gateway's capability to collect and forward data by creating external data destinations and custom collection jobs.

Table 2: Tasks to Complete to Set Up Cisco Crosswork Data Gateway to Collect Data

Task	Follow the steps in...
1. Create Crosswork Data Gateway pools.	Create a Cisco Crosswork Data Gateway Pool, on page 9
2. Attach devices to Crosswork Data Gateway.	Attach Devices to a Crosswork Data Gateway, on page 14
3. Verify that the default collection jobs are created and running successfully.	Monitor Collection Jobs, on page 75
4. (optional) Extend device coverage to collect data from currently unsupported devices or third-party devices.	Manage Device Packages, on page 32
5. (optional) Forward data to external data destinations.	Create and Manage External Data Destinations, on page 26
6. (optional) Create custom collection jobs (outside of those built for you by Cisco Crosswork).	Manage Crosswork Data Gateway Collection Jobs, on page 39

# Crosswork Data Gateway High Availability with Pools

A Cisco Crosswork Data Gateway pool ensures that your devices are managed and collections occur with minimal disruption.

A pool can consist of one or more Cisco Crosswork Data Gateway instances with an option to enable high availability.

If a Crosswork Data Gateway instance in the pool goes down, Cisco Crosswork automatically replaces that instance with a standby instance from the pool (failover) or let you manually initiate a failover. For information on how to initiate a failover, see .

A Crosswork Data Gateway instance that has the **Operational state** as **Error** and is part of a pool that is **Protected** is eligible for failover. Devices and any existing collection jobs are assigned automatically from the failed instance to the standby instance. Once the instance that went down becomes operational, it becomes a standby instance in the pool.

Figure 2: Crosswork Data Gateway High Availability
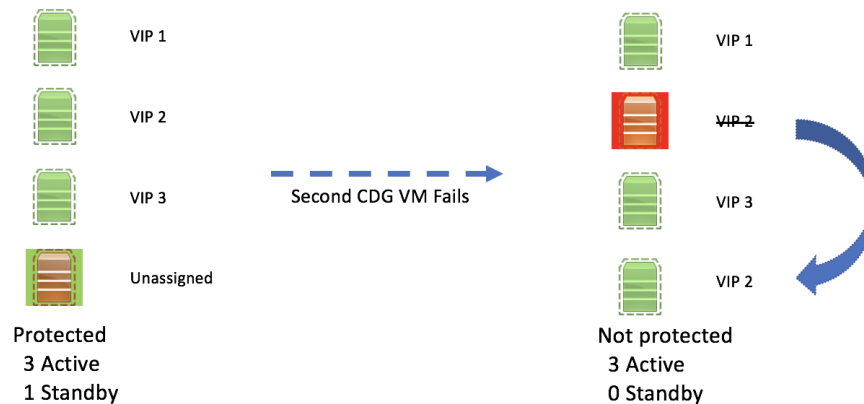
Note   If more than one Crosswork Data Gateway instance in a pool has same Southbound IP address, reboot the standby Crosswork Data Gateway, so that the standby Crosswork Data Gateway instance loses its southbound IP address once it comes up.

For example, CDG1 (Active) with southbound IP address IP1 goes down. Cisco Crosswork replaces CDG1 with CDG2(Standby) as new active and programs the same IP1 as southbound IP on CDG2. CDG1 later comes up and becomes the new standby in the pool, but retains the same IP1 as its southbound IP address. This results in both CDG1 and CDG2 having same IP1 as southbound IPs.

A Crosswork Data Gateway pool has following states:

- **Protected**: All instances are UP and there is at least one standby instance in the pool.

- **Not Protected**: All the standby instances are DOWN and there are none available to replace a instance that is in use.

- **Limited Protection**: Some standby instances are DOWN, but there is still at least one standby that is UP.

- **None Planned**: No standby instances were added to the pool during pool creation.

The **Operational state** of the Data Gateway is considered to be in the **Error** state if the Data Gateway has failed to report its health for 3 consecutive vitals cycles (30 seconds). This failure in reporting health may be due to:

- Issues in the Data Gateway instance. For example, the Data Gateway has run out of resources to report the health.

- Network issues between Cisco Crosswork and Crosswork Data Gateway.

The **Operational state** of the Crosswork Data Gateway is checked every 20 seconds. If the active instance is in the **Error** state, a failover is triggered, and the spare instance in the pool becomes the active instance in the pool.

Enable FQDN for Secure Syslog Communication

Crosswork Data Gateway supports secure syslog communication to devices which require the syslog certificate to contain the host name or Fully Qualified Domain Name (FQDN) instead of the virtual IP address of the Crosswork Data Gateway. This is an optional feature that can be enabled for devices which mandate having the host name or FQDN in the syslog certificate. If enabled, Cisco Crosswork fetches the host name or FQDN for each virtual IP address of the Crosswork Data Gateway from the DNS server. FQDNs for newly added virtual IP(s) will be fetched after you save the pool. The syslog certificate will then contain the FQDN in the CN and SAN instead of the virtual IP address of the Crosswork Data Gateway. For details on how to configure secure syslog on devices, see Configure Secure Syslog on Device, on page 56.

Note Crosswork Data Gateway pools can be created without enabling FQDN in which case the syslog certificate contains virtual IP addresses of the Crosswork Data Gateway. You can always edit the pool later to enable or disable FQDN to switch between having FQDNs or virtual IP addresses in the syslog certificate.

When the FQDN values are updated in the DNS server, you must refresh the FQDN values for virtual IP(s) in the pool.

To refresh FQDN, in the **Pools** tab, navigate to the pool for which you want to refresh the FQDN. In the **Actions** column, click the (…) icon and select **Refresh FQDN**.

Create a Cisco Crosswork Data Gateway Pool

When you create a Cisco Crosswork Data Gateway pool, follow these guidelines:

- You must create at least one pool and assign Crosswork Data Gateway instances to it. This step is mandatory to set up the Crosswork Data Gateway for collection.

- All the Crosswork Data Gateway instances in a pool need to be of the same configuration (either Standard, or Extended).

- If you have deployed the VMs on Amazon EC2, all the Crosswork Data Gateway instances in a pool must be from the same availability zone.

To create a Crosswork Data Gateway pool:

Before you begin

Before creating a Cisco Crosswork Data Gateway pool:

- Decide if you wish to enable high availability for the pool.

- Ensure that you have installed all Crosswork Data Gateway instances that you wish to add to the pool.

- Ensure that you are familiar with the pool types:

  - L2 Stretch: The pool in which the network devices connect to CDG instances that are part of a HA pool residing on a single IP subnet. The subnet can be intra-DC (Data Center) or extended inter-DC.

  Note The L2 Stretch pool type is not supported when creating pools in the Amazon EKS environment.

  - L3 with Load Balancer: The pool in which the network devices connect to CDGs that reside across multiple different subnets which are part of the same HA pool. This configuration requires an external Network Load Balancer (NLB) to host a VIP towards the network devices while shielding the internal subnet addresses of the CDG HA pool.

- Confirm that the Operational State of the Crosswork Data Gateway instances is **Not Ready**.

- Have network information such as virtual IP address (one virtual IP for each active data gateway), subnet mask and gateway information ready.

  Note Gateway is only required when using 3 NICs.

  Depending on the number of vNICs in your deployment, the virtual IP address would be:

  - An additional IP address on the Management Network in a single NIC deployment.

  - An additional IP address on the Data Network for 2 NIC deployment.

  - An IP address on the Southbound Network for 3 NICs deployment.

  These virtual IP addresses must be planned in advance during the network design phase.

- Decide if you wish to enable Fully Qualified Domain Name (FQDN) for virtual IP(s) addresses in the pool. If yes, ensure that you have configured FQDN for virtual IP(s) in the DNS server to create the pool successfully.

Step 1 From the main menu, choose **Administration** > **Data Gateway Management** and click the **Pools** tab.

Step 2 In the **Pools** tab, click the ⊞ button and select **L2 Stretch** or **L3 with Load Balancer**. For information on the pool types, on the top-right, click **Types of Pools**.

Figure 3: Pools Window
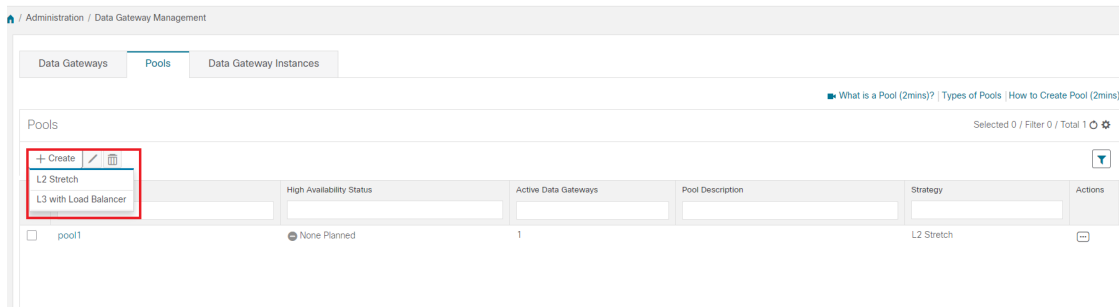
The **Create Pool** page opens.

Step 3   In the **Pool Parameters** pane, enter the values for the following parameters:

- **Pool Name**: Name of the pool that suitably describes the network.

- **Description**: A description of the pool.

Step 4   In the **Pool Resources** pane, add the following details:

Depending on the pool type, the pool resources parameters change. For example, for L2 Stretch the pool resources consider the IPv4 addresses.

- **IPv4** or **IPv6**: Select either an IPv4 or IPv6 address family for virtual IPs. The following parameters are required for IP addresses:

    - **Subnet**: Subnet mask for each Cisco Crosswork Data Gateway. IPv4 subnet mask ranges from 1 to 32 and port range from 1024 to 65535.

    - **Network Gateway**: Gateway address for each Cisco Crosswork Data Gateway to communicate with the devices.

    - (Optional) **Enable FQDN for Virtual IP address**: Select this option to use hostname or Fully Qualified Domain Name (FQDN) for each virtual IP address of the Crosswork Data Gateway in the syslog certificate.

- **FQDN**: Fully Qualified Domain Name (FQDN) for each virtual IP address of the Crosswork Data Gateway in the syslog certificate.

- **Add Another**: Based on the address family you chose earlier (IPv4 or IPv6, FQDN), enter a virtual IP address or FQDN for every active Cisco Crosswork Data Gateway instance.

- **Add the number of standby data gateways desired for protection**: Entering a value greater than 0 in this field enables high availability for the pool. When an active data gateway goes down, a 'standby' in the pool replaces it to ensure protection.

    The number of Crosswork Data Gateway instances you add to the pool should be equal to the total number of virtual IPs and standby Crosswork Data Gateway instances. For example, if you have entered 3 virtual IPs and wish to have 2 standby instances, add 5 Cisco Crosswork Data Gateway instances to the pool.

- **Select and add Data Gateway Instance resources to pool**: Select Data Gateway instances from the **Unassigned Data Gateway Instance(s)** on the left and click right arrow to move the instances to the **Data Gateway Instance(s) Added to Pool**.

Figure 4: Create Pool Window

Step 5   Click **Save**.

After you click **Save**, a virtual Crosswork Data Gateway gets created automatically and is visible under the **Data Gateway Instances** tab. Attach devices to this virtual Crosswork Data Gateway to run collection jobs.

Note   Pool creation fails if the FQDN configurations are missing for virtual IP(s) in the DNS server. Either check FQDN configuration in the DNS server or disable the FQDN option and try again.

Assign Data Gateway to Geo Redundancy-enabled Sites

You can assign data gateways to either Active or Standby site.

Before you begin

Ensure that you are aware of the following:

- The data gateway instances can be assigned to sites only with the Geo Redundancy feature is enabled. For information on how to enabled the Geo Redundancy capabilities, see the *Enable Geo Redundancy* section in *Cisco Crosswork Network Controller 6.0 Installation Guide*.

- When the data gateways are in the unassigned state, you have the option to assign them to either an Active or Standby site.

- If the data gateway is a member of a pool, you can assign it to a site only during Crosswork migration using the edit pool option. During the Crosswork migration, a notification is shown on the **Data Gateway Management** page, to indicate the ongoing migration.

Step 1   From the main menu, choose **Administration** > **Data Gateway Management** and click the **Data Gateway Instances** tab.

Step 2   Click **Assign DG Instance to Site**. The **Assign Data Gateway Instance(s) to Site** window opens. The window displays the data gateway instances in the unassigned state.

Step 3   Select the data gateway instance that you want to change the assigned site.

Step 4   Click the **Select Site** drop-down and select the site.

Step 5   Click **Assign**.

A message appears confirming that data gateway instance is assigned to the selected site. The **Site Name** column on the **Administration** > **Data Gateway Management** and click the **Data Gateway Instances** tab displays the changed site name.

Perform a Manual Failover

When you have a planned maintenance schedule, you can enforce a failover from an instance to a standby instance residing within the same pool.

Before you begin

Before initiating a failover in a Crosswork Data Gateway pool, note the following:

- Manual failover cannot be attempted on a data gateway for which the autofailover is in-progress.

- Crosswork regards only one failover request at a time. It does not support multiple failover requests at the same time.

- Confirm that at least one instance has the operational state as **UP** or **NOT_READY**. Crosswork considers this instance as the standby on which the failover happens.

- Minimum one standby data gateway instance must be in the **NOT_READY** state.

- A data gateway in the maintenance mode cannot be used as a spare for the future failover procedures until its operational state as **UP**.

- The spare data gateway instance that you plan on using for failover must be in the **NOT_READY** state.

Follow the steps below to initiate a manual failover of the Crosswork Data Gateway instance:

Step 1   From the main menu, choose **Administration > Data Gateway Management > Data Gateways** tab.

Step 2   For the Crosswork Data Gateway from which you want to initiate a failover, under **Actions** column, click, and select **Initiate Failover**.

Step 3   In the **Warning** window, if you want to move the selected data gateway to the maintenance mode after the failover is complete, select the check box.

Step 4   Click **Continue**.

What to do next

If the failover is not complete due to database connectivity or OAM channel issues, reattempt the failover after confirming you have at least standby instance in the **NOT_READY** state.

Before initiating a subsequent failover, wait for 10-30 seconds for the standby data gateway to move to the **NOT_READY** state. If the standby instance remains in the **UP** state after 30 seconds, restart the oam-manager of the data gateway to restore the operational state as **NOT_READY**.

Attach Devices to a Crosswork Data Gateway

Follow these guidelines when you attach devices to a Crosswork Data Gateway.

- A device can be attached to only one Crosswork Data Gateway.

- For optimal performance, we recommend attaching devices to a Crosswork Data Gateway in batches of 300 devices or fewer.

> **Note** Crosswork Data Gateway does not support the usage of older unsecure key exchange algorithms (KEX), as it can result in SSH connection failure.

Before you begin

Ensure that the **Admin state** and **Operational state** of the Crosswork Data Gateway to which you want to attach devices is **Up**.

Step 1 (Optional) Before attaching devices to an existing Crosswork Data Gateway, we recommend that you check the health of the Crosswork Data Gateway. See Monitor Crosswork Data Gateway Health, on page 15 for more information.

Step 2 From the main menu, navigate to **Administration** > **Data Gateway Management** > **Data Gateways**.

Step 3 For the Crosswork Data Gateway to which you want to attach devices, in **Actions** column, click ⋯ and select **Attach Devices**. The **Attach Devices** window opens showing all the devices available for attaching.

Figure 5: Attach Devices Window
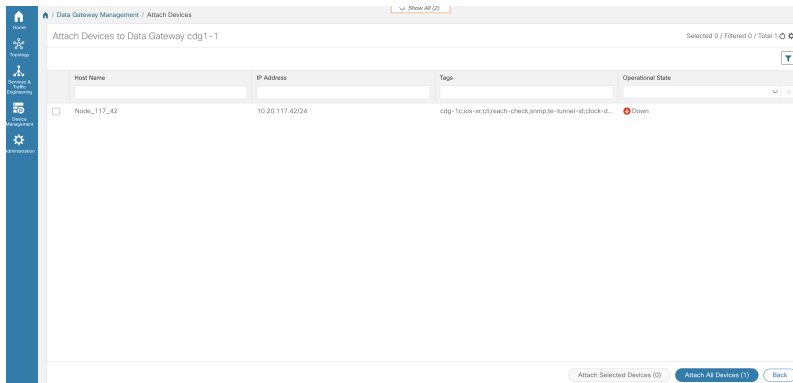
Step 4 To attach all the devices, click **Attach All Devices**. Otherwise, select the devices you want to attach and click **Attach Selected Devices**.

Step 5 In **Confirm - Attach Devices** dialog, click **Attach**.

Verify that your changes are successful by checking the **Attached Device Count** column in the **Data Gateways** pane.

Monitor the Crosswork Data Gateway health to ensure that the Crosswork Data Gateway is functioning well with the newly attached devices. For information on how to monitor the heath, see Monitor Crosswork Data Gateway Health, on page 15.

Manage Crosswork Data Gateway Post-Setup

This section explains various maintenance tasks within the Crosswork Data Gateway.

Monitor Crosswork Data Gateway Health

You can view the operations and health summary of a Crosswork Data Gateway from the Crosswork Data Gateway vitals page at **Administration** > **Data Gateway Management** > **Data Gateways** > **(click){Crosswork Data Gateway}**. This page also has details of the health of various containerized services running on the Crosswork Data Gateway. The overall health of Crosswork Data Gateway also depends on the health of each containerized service.

You can perform the troubleshooting activities, by clicking on the **Actions** button and selecting the appropriate menu:

- **Ping** – Checks the reachability to any IP address.

- **Trace Route** – Helps troubleshoot latency issues. This option provides you a rough time estimate for the Crosswork Data Gateway to reach the destination.

- **Download Service Metrics** – Downloads the metrics for all collection jobs for a Crosswork Data Gateway from the Cisco Crosswork UI.

- **Download Showtech** – Downloads the showtech logs from Cisco Crosswork UI.

- **Change Log Level** – Allows you to change the log level of a Crosswork Data Gateway's components, for example collectors (cli-collector) and infra services (oam-manager). Log level changes apply only to the Crosswork Data Gateway on which you are making the change.

Figure 6: Data Gateway Window
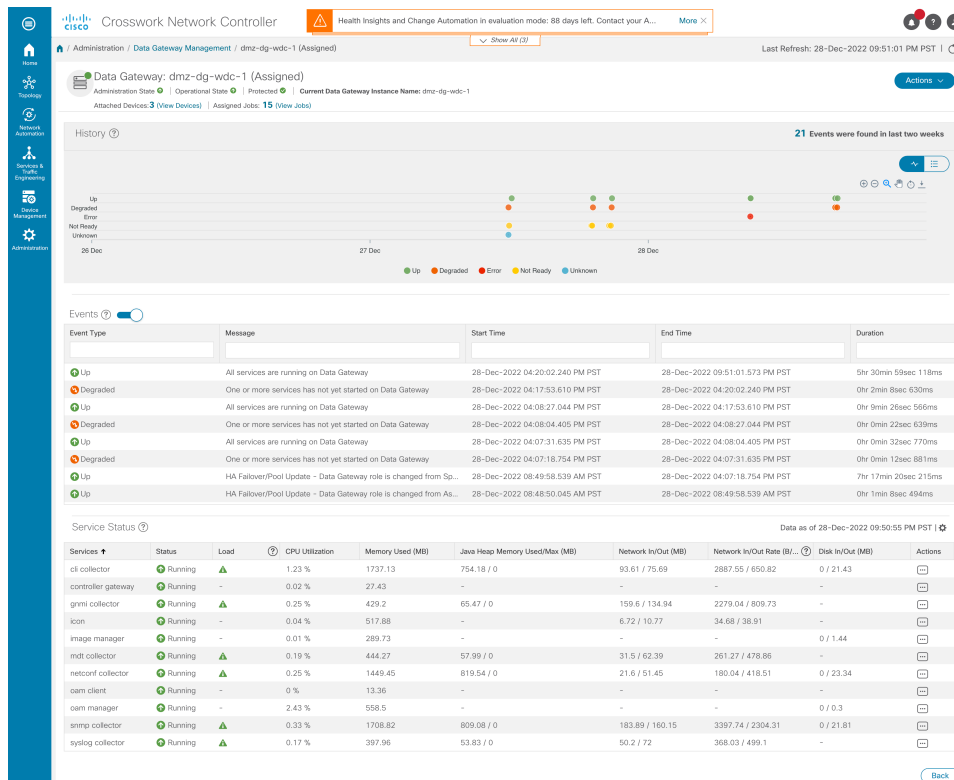
The following parameters are displayed on this page:

- **General Cisco Crosswork Data Gateway Details** – Displays general details of the Crosswork Data Gateway including operational state, high availability state, attached device count, and assigned jobs. The **Actions** option lists the various troubleshooting options that are available from the UI.

- **History** – Shows the outage history chart of the Cisco Crosswork Data Gateway over 14 days including timestamp, outage time, and clear time. Use the options in the top-right corner of the pane to zoom in, zoom out, pan, or download the SVG and PNG of the history chart of a specific time period within the graph.

- **Events** – Displays a list of all Cisco Crosswork Data Gateway transition state changes over the last 14 days. It includes information such as the event details, including operational state changes, role changes, a message indicating the reason for the status change, timestamp, and duration.

- **Health** – Shows the health information of the Cisco Crosswork Data Gateway. The timestamp in the top-right corner is the timestamp when the last health data was collected. If the Crosswork Data Gateway is in an **Error** state or if the data is stale for any reason, the timestamp label highlights that the data is old. If the **CPU Utilization** of a Crosswork Data Gateway exceeds 80%, we recommend taking corrective action before the **CPU Utilization** increases further leading to failure of the Crosswork Data Gateway.

  The **Network In/Out** section displays the speed at which the vNICs sent and receive the network data.

  You can view the interface roles assigned to the vNICs by clicking on the *?* icon next to **Additional Role Information**. The popup provides information about the available roles.

Figure 7: Crosswork Data Gateway Health Window
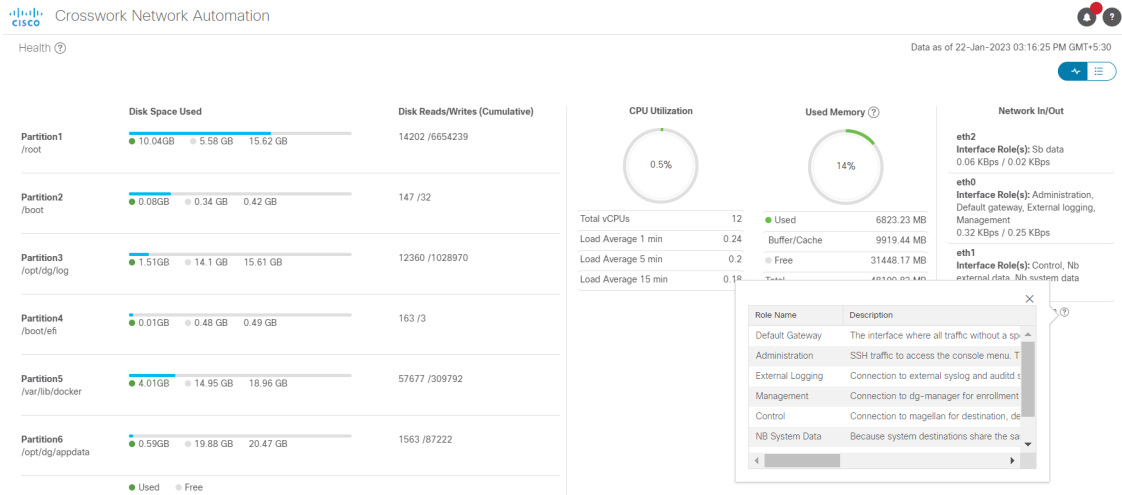
- **Service Status** – Displays the health information of the individual container services running on the Crosswork Data Gateway and their resource consumption with an option to restart (**Actions > Restart**) an individual service. The Load column indicates the processing load of that specific collector/service. The load score of a collector is calculated using several metrics. The load scores are mapped with low, medium, or high severity zones. A collector that is consistently operating in the **High** zone means that the collector has reached peak capacity for the given CPU/Memory resource profile. For more information on how the load score is calculated, see Load Score Calculation.

Note

The list of container services differs between Standard Crosswork Data Gateway and Extended Crosswork Data Gateway. Extended Crosswork Data Gateway has more containers installed.

The resource consumption data that is displayed is from docker statistics. These values are higher than the actual resources consumed by the containerized service.

Figure 8: Service Status Window

We recommend monitoring the health of the Crosswork Data Gateways in your network periodically to prevent overloading and take corrective actions, such as adding additional resources or reducing load on the Crosswork Data Gateway well in time proactively.

1. The DG-Manager generates alarms when Crosswork Data Gateway fails or is reaching the resource capacity limits. You can review the alarm details through **Crosswork UI > Showtech Requests** or by logging in to the Alarm pods.

   The alarms include the event title, severity, the configuration stage (Day 0, 1, or 2), description, and the remediation action. For more information on how to navigate to the **Showtech Requests** window, see

2. If the **CPU Utilization** of a Crosswork Data Gateway exceeds 80%, we recommend that you do not create more collection jobs until you have reduced the **CPU Utilization** by moving devices to another CDG or have added other VMs to the pool or the increased the cadence of existing collection jobs.

3. If the **CPU Utilization** of a Crosswork Data Gateway exceeds 90%, we recommend that you move devices to another Crosswork Data Gateway that has a lower **CPU Utilization** percentage.

4. We recommend that you check the system alarms weekly. Investigate to confirm it is not because of a resource problem and data drops are not frequent. Then fix issues on the data destinations or increase cadence of the collection job.

Viewing Crosswork Data Gateway Alarms

Crosswork Data Gateway generates an alarm when it detects an anomaly that prevents data collections. You can review the alarms to understand the issue affecting data collection, and take the remediation action, if required.

To view the alarms, navigate to the Crosswork UI:

Note Alternatively, you can log in to the alarms pod and view the alarms in the DgManager.yaml file.

Step 1 From the main menu, choose **Administration** > **Crosswork Manager** > **Application Management** tab and click **Applications**.

Step 2 In the **Platform Infrastructure** tile, click **View Details**. The **Application Details** window opens.

Step 3 In the **Microservices** tab, type alarms in the **Name** field to locate the alarm pod. The status of the alarm pod must be healthy.

Step 4 Click the icon under **Actions** and select **Showtech Requests**. The **Showtech Requests** window displays the details of the showtech jobs.

Step 5 (Optional) Log in to the alarm pod and view the alarms or download the alarms by clicking **Publish** to publish the showtech logs. The **Enter Destination Server** dialog box is displayed. Enter the relevant details and click **Publish**.

Figure 9: Showtech Requests Window

Enter Destination Server   ✕

      File Selected to Publish

      Server Path/Location *

      Host Name/IP Address *

      Port *

      Username *

      Password *

                                    Publish   Cancel

The alarms are published at the destination that you have provided.

Manage a Crosswork Data Gateway Pool

Follow the steps to edit or delete a Cisco Crosswork Data Gateway pool. To create a pool, see Create a Cisco Crosswork Data Gateway Pool, on page 9.

Before you begin

Important points to consider before you edit or delete the pool:

- Virtual data gateways or pools that have devices attached cannot be deleted.

- A date gateway instance can be removed from the pool only when all the mapped devices are unmapped from Crosswork Data Gateway. When a Crosswork Data Gateway instance is removed from the pool, a standby instance from the same pool becomes its replacement after you perform a failover procedure. For information about manual failovers, see Perform a Manual Failover, on page 13.

- Before you delete a Crosswork Data Gateway pool, detach devices from the Crosswork Data Gateway first or move the devices to another Crosswork Data Gateway.

Step 1   From the main menu, choose **Administration** > **Data Gateway Management** and click **Pools** tab.

Step 2   **Edit a Crosswork Data Gateway Pool**:

a) Select the pool which you wish to edit from the list of pools that is displayed in this page.

b) Click ✎ button to open **Edit High Availability (HA) Pool** page.

When you edit a resource pool, you can only change the parameters in the **Pool Resources** pane. You cannot edit the parameters in the **Pool Parameters** pane. To make changes to the parameters in the **Pool Parameters** pane, create a new pool with the desired values and move the Cisco Crosswork Data Gateway instances to that pool.

Figure 10: Data Gateway Management - Edit HA Pool Window

c) In the **Pool Resources** pane, you can modify the resource parameters that change depending on the pool type:

• Add and delete a virtual IP address or FQDN for every active data gateway needed.

• Change the number of standby Crosswork Data Gateway instances.

• Add and remove Crosswork Data Gateway instances from the pool.

• Enable or disable FQDN for the pool.

d) Click **Save** after you have completed making your changes.

Step 3 **Delete a Crosswork Data Gateway Pool**:

a) Select the pool that you want to delete and click [🗑].
b) Click **Delete** in the **Delete High Availability (HA) Pool** window to delete the pool.

Manage Cisco Crosswork Data Gateway Device Assignments

Follow these guidelines when you move or detach devices from a Crosswork Data Gateway.

• A device can be attached to only one Crosswork Data Gateway.

• When moving devices to a Crosswork Data Gateway in different pool, ensure that the Gateway of the pool is same as the Gateway of the current pool. Moving devices to a Crosswork Data Gateway with mismatching Gateway results in failed collections.

• Detaching a device from Cisco Crosswork Data Gateway deletes all collection jobs corresponding to the device. If you do not want to lose the collection jobs submitted for the device you wish to detach, move the device to another Cisco Data Gateway instead.

Follow the steps below to move or detach devices from a Crosswork Data Gateway pool. To add devices to the pool, see Attach Devices to a Crosswork Data Gateway, on page 14.

Step 1   From the Cisco Crosswork Main Menu, navigate to **Administration** > **Data Gateway Management** > **Data Gateways**.

Figure 11: Data Gateways Window

Step 2   **Move Devices**:

a)   For the Crosswork Data Gateway from which you want to move devices, under the **Actions** column, click ⋯ and select **Move Devices**. The **Move Attached Devices** window opens showing all the devices available for moving.

b)   From the **To this Data Gateway** drop down, select the data gateway to which you want to move the devices.

Figure 12: Move Attached Devices Window

c) To move all the devices, click **Move All Devices**. Otherwise, select the devices you want to move and click **Move Selected Devices**.

d) In the **Confirm - Move Devices** window, click **Move**.

Step 3   **Detach Devices**:

a) For the Crosswork Data Gateway from which you want to detach devices, under the **Actions** column, click ⋯ and select **Detach Devices**. The **Detach Devices** window opens showing all attached devices.

Figure 13: Detach Devices Window

b) To detach all the devices, click **Detach All Devices**. Otherwise, select the devices you want to detach and click **Detach**

c) In the **Confirm - Detach Devices** window, click **Detach**.

Verify that your changes are successful by checking the **Attached Device Count** under the **Data Gateways** pane. Click the ⓘ icon next to the attached device count to see the list of devices attached to the selected Crosswork Data Gateway.

For information on how initiate a failover, see Perform a Manual Failover, on page 13.

Maintain Crosswork Data Gateway Instances

This section explains the maintenance tasks of the Crosswork Data Gateway instance.

Change the Administration State of Cisco Crosswork Data Gateway Instance

To perform upgrades or other maintenance within the data center is may become necessary to suspend operations between Cisco Crosswork platform and the Cisco Crosswork Data Gateway. This can be done by placing the Cisco Crosswork Data Gateway into **Maintenance** mode. During downtime, the administrator can modify Cisco Crosswork Data Gateway, such as updating the certificates, and so on.

Note	If the maintenance activities are affecting the communication between Crosswork and Crosswork Data Gateway, the collection is interrupted and resumes when the communication is restored. Similarly if the maintenance activities are affecting the communication between Crosswork Data Gateway and external destinations (Kafka/gRPC), the collection is interrupted and resumes when the communication is restored.

After the changes are complete, the admin can change the administration state to **Up**. Once the Crosswork Data Gateway instance is up, Cisco Crosswork resumes sending jobs to it.

Note	In the **Assigned** state, a data gateway cannot be switched directly to the maintenance mode. To enter the maintenance mode, you must either execute a manual failover when standby is available or remove the data gateway from the pool. See Perform a Manual Failover, on page 13 for information on manual failover.

Use the following steps to change the administration state of a Crosswork Data Gateway instance:

Before you begin

You cannot move a data gateway to **Maintenance** mode if the role is assigned, which indicates that the data gateway is active in a pool. However, the gateway can be assigned the following roles:

- Spare role when a manual or autofailover occurs.
- Assigned role when it is the only gateway in the pool.

Step 1   From the main menu, choose **Administration** > **Data Gateway Management** > **Data Gateway Instances**.

You can also navigate to the Crosswork Data Gateway details page that displays the operations and health summary of an instance by clicking the Data Gateway instance or pool name in the table. Clicking on the ⓘ next to Data Gateway instance name displays the enrollment details that includes interface role details.

Step 2   For the Cisco Crosswork Data Gateway whose administrative state you want to change, click ⋯ under **Actions** column.

Figure 14: Data Gateway Instances Window

Step 3   Select the administration state to which you want to switch to.

Delete Crosswork Data Gateway Instance from Cisco Crosswork

Follow the steps below to delete a Cisco Crosswork Data Gateway instance from Cisco Crosswork:

Before you begin

It is recommended that you move the attached devices to another data gateway to not lose any jobs corresponding to these devices. If you detach the devices from Cisco Crosswork Data Gateway instance, then the corresponding jobs are deleted.

Step 1   From the main menu, choose **Administration** > **Data Gateway Management** > **Data Gateway Instances**.

Step 2   For the Crosswork Data Gateway that you want to delete, click ⋯ under **Actions** column and click **Delete**.

Figure 15: Data Gateway Instances Window
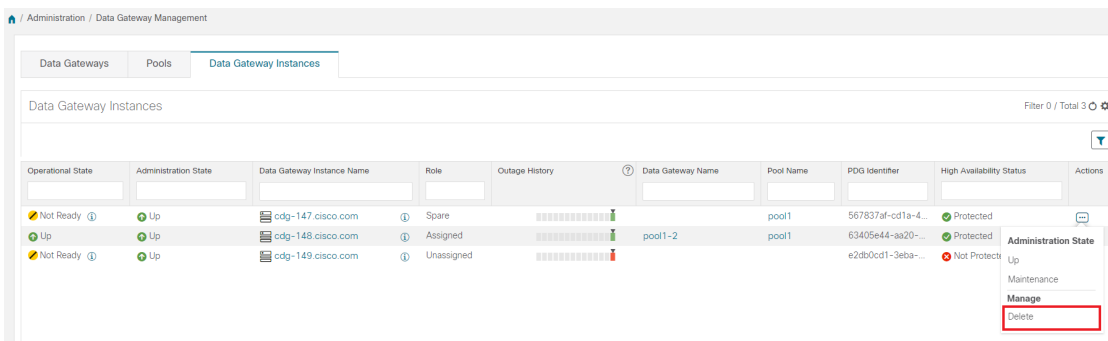
Step 3   The Cisco Crosswork Data Gateway instance must be in maintenance mode to be deleted. Click **Switch to maintenance & continue** when prompted to switch to **Maintenance** mode.

Figure 16: Switch to maintenance & continue Pop-up Window
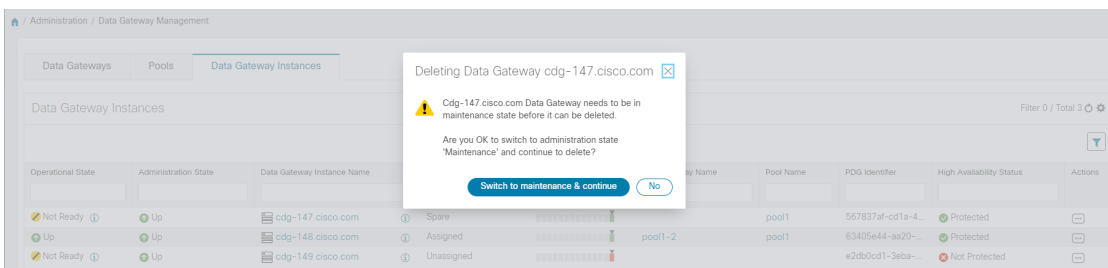
Step 4   Check the check box for **I understand the concern associated with deleting the Data Gateways** and click **Remove CDG**.

Figure 17: Delete Data Gateway Confirmation Dialog Box
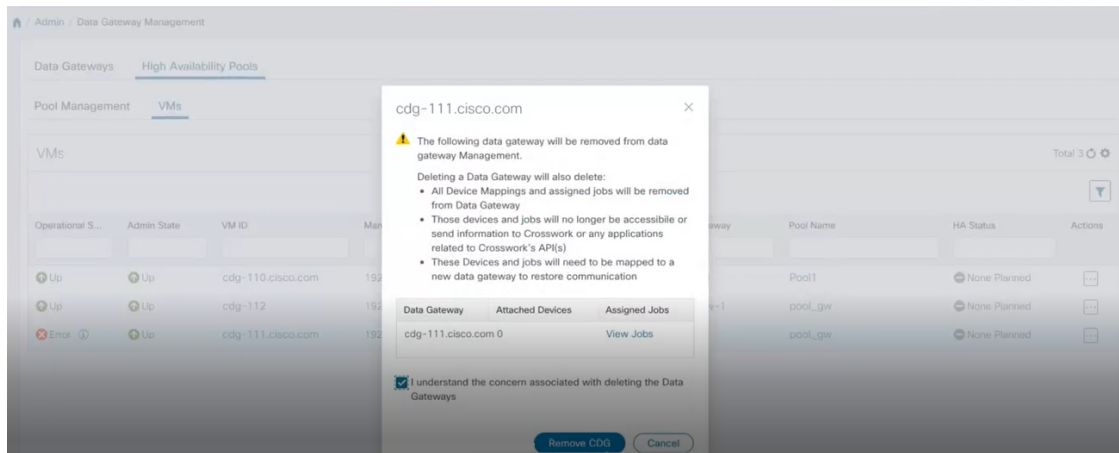
Redeploy a Crosswork Data Gateway Instance

To redeploy a Crosswork Data Gateway instance, delete the old instance and install a new one. For details on how to install a new Crosswork Data Gateway instance, see *Cisco Crosswork Network Controller 5.0 Installation Guide*.

If you are redeploying the Crosswork Data Gateway instance in order to change the deployment profile of the instance (for example, change the profile from Standard to Extended), ensure that you manually rollback any Data Gateway global parameter changes before attempting to redeploy the Crosswork Data Gateway instance.

Important points to consider

1. If the Crosswork Data Gateway instance was already enrolled with Cisco Crosswork and you have installed the instance again with the same name, change the **Administration State** of the Crosswork Data Gateway instance to **Maintenance** for auto-enrollment to go through.

2. If a Crosswork Data Gateway instance was already enrolled with Cisco Crosswork and Cisco Crosswork was installed again, re-enroll the existing Crosswork Data Gateway instance with Cisco Crosswork.

   See Re-enroll Crosswork Data Gateway.

Configure Crosswork Data Gateway Global Settings

This section describes how to configure global settings for Cisco Crosswork Data Gateway. These settings include:

- Manage Device Packages, on page 32

- Configure Crosswork Data Gateway Global Parameters, on page 35

- Allocate Crosswork Data Gateway Resources, on page 37

Create and Manage External Data Destinations

Cisco Crosswork allows you to create external data destinations (Kafka or external gRPC) that can be used by collection jobs to deposit data.

It can be accessed by navigating to **Administration** > **Data Gateway Global Settings** > **Data Destinations**. You can add a new data destination, update the settings configured for an existing data destination, and delete a data destination.

The table in the **Data Destinations** page lists the approved data destinations that can be used by the collection jobs to deposit their data.

Note	The **Crosswork_Kafka** and **cd-astack-pipeline** are internal data destinations and cannot be updated or deleted.

Figure 18: Data Destinations Window

The UUID is the Unique identifier for the data destination. Cisco Crosswork automatically generates this ID when an external data destination is created. When creating collection jobs using the Cisco Crosswork UI the destination for the data is selected using a drop-down list of the configured destinations. When creating a collection job via the API, you will need to know the UUID of the destination where the collector is to send the data it collects.

To view details of a data destination, in the Data Destinations pane, click ⓘ icon next to the data destination name whose details you want to see.

Licensing Requirements for External Collection Jobs

To be able to create collection jobs that can forward data to external data destinations, ensure that you meet the following licensing requirements:

1. From the main menu, go to **Administration** > **Application Management** > **Smart License**.

2. Select **Crosswork Platform Services** in the application field.

3. Ensure that the status is as follows:

   - **Registration Status - Registered**

     Indicates that you have registered with Cisco Smart Software Manager (CSSM) and are authorized to use the reserved licensed features.

> • **License Authorization Status** - **Authorized** (In Compliance).
>
> Indicates that you have not exceeded the device count in the external collection jobs.
>
> • Under Smart Licensing Usage, **CW_EXTERNAL_COLLECT** has status as **In Compliance**.

If you do not register with Cisco Smart Software Manager (CSSM) after the Evaluation period has expired or you have exceeded the device count in external collection jobs (**License Authorization Status** is **Out of Compliance**), you will not be able to create external collection jobs. However, you can still view and delete any existing collection jobs.

Add or Edit a Data Destination

Follow the steps below to add a new data destination. You can then use this data destination to forward data to. You can add multiple data destinations.

Few points to note when adding an external data destination are:

- If you reinstall an already existing external Kafka data destination with the same IP address, then the collectors need to be restarted for changes to take effect.

- You can secure the communication channel between Cisco Crosswork and the specified data destination that is, either Crosswork Kafka or external Kafka. (See **Step 6** in this procedure). However, enabling security can impact performance.

- If your external data destination requires a TLS connection, keep the public certificate ready or if it requires client authentication, keep the client certificate and key files ready. The client key might be password-encrypted which needs to be configured as part of the data destination provisioning. Currently, Crosswork Data Gateway supports IP-based certificates only.

- Ensure that the certificates are PEM encoded and the key file is in PKCS#8 format when generating them with your Certificate Authority.

- Ensure that you create the Kafka topics before you submit the job in Cisco Crosswork. Depending on the external Kafka and how topics are managed in that external Kafka, Cisco Crosswork logs may show the following exception if the topic does not exist at the time of dispatching the collected data to that specific external Kafka / topic. This could be because the topic is not created yet or the topic was deleted before the collection job was complete.

```
destinationContext: topicmdt4
org.apache.kafka.common.errors.UnknownTopicOrPartitionException: This server does not
host this topic-partition.
```

- Check and validate the port connectivity for the data destination. If the port is unreachable in the destination, it leads to a failed collection.

- Crosswork Data Gateway allows you to configure custom values in the destination properties for a Kafka destination (see Step 4 in this procedure).

> **Note**   This feature is not supported on a gRPC destination.

- Global properties entered in the **Destination Details** pane are mandatory and will be applied to the Kafka destination by default unless there are custom values specified at the individual collector level. Custom values that you specify for a collector apply only to that collector.

- The external destination must be IPv4 or IPv6 depending on the protocol specified when deploying Crosswork Data Gateway. For instance, if IPv4 was chosen during the deployment, the external destination should also be IPv4.

- Modifications to the hostname and IP address mapping reflect on Crosswork Data Gateway only after the duration configured in the Time to Live (TTL) field on the DNS server is completed. If you want the change to reflect immediately, we recommend rebooting the VM.

Before you begin

If you are using an external Kafka server for data collection, ensure the following:

- You have configured the following properties on the external Kafka server:

Note Refer to *Kafka documentation* for description and usage of these properties as this explanation is out of scope of this document.

  - `num.io.threads = 8`

  - `num.network.threads = 3`

  - `message.max.bytes= 30000000`

- You have created Kafka topics that you want to be used for data collection.

- Ensure that 'reachability-topic' is configured on the Kafka destination before a new collection job is started. This configuration is required for monitoring the health of the Kafka destination.

Step 1 From the main menu, choose **Administration** > **Data Gateway Global Settings** > **Data Destinations**.

Step 2 In the **Data Destinations** page, click ⊞ button. The **Add Destination** page opens.

If you want to edit an existing destination, click ✏ button to open **Edit Destination** page and edit the parameters.

Note Updating a data destination causes the Cisco Crosswork Data Gateway using it to reestablish a session with that data destination. Data collection will be paused and resumes once the session is reestablished.

Step 3 Enter or modify the values for the following parameters:

Field	Value	Available in gRPC	Available in Kafka
Destination Name	Enter a descriptive data destination name. The name can contain a maximum of 128 alphanumeric characters, plus underscores ("_") or hyphens ("-"). No other special characters are allowed. If you have many data destinations, make the name as informative as possible to be able to distinguish later.	Yes	Yes

Field	Value	Available in gRPC	Available in Kafka
Server Type	From the drop-down, select the server type of your data destination.	Yes	Yes
Encoding	From the drop-down, select the encoding (json or gpbkv).	Yes	Yes
Compression Type	From the drop-down, select the compression type.	Yes Supported compression types are Snappy, gzip, lz4, zstd, and none. **Note** zstd compression type is supported only for Kafka 2.0 or higher.	Yes Supported compression types are Snappy, gzip, and deflate.
Dispatch Type	This field is available when the **Server Type** field is set to **gRPC**. From the drop-down, select the dispatch method as stream or unary. Crosswork Data Gateway transmits the collected data to the destination as data streams or unary. The default value is unary.	Yes	No
Maximum Message Size (bytes)	Enter the maximum message size in bytes. • **Default Value**: 100000000 bytes/ 30 MB • **Min**: 1000000 bytes/1 MB • **Max**: 100000000 bytes/ 30 MB	No	Yes
Buffer Memory	Enter the required buffer memory in bytes. • **Default Value**: 52428800 bytes • **Min**: 52428800 bytes • **Max**: 314572800 bytes	No	Yes

Field	Value	Available in gRPC	Available in Kafka
Batch Size (bytes)	Enter the required batch size in bytes. • **Default Value**: 6400000 bytes/6.4 MB • **Min**: 16384 bytes/ 16.38 KB • **Max**: 6400000 bytes/6.4 MB	No	Yes
Linger (milliseconds)	Enter the required linger time in milliseconds. • **Default Value**: 5000 ms • **Min**: 0 ms • **Max**: 5000 ms	No	Yes
Request Timeout	Enter the duration that the request waits for a response. After the configured duration is met, the request expires. • **Default Value**: 30 ms • **Min**: 30 ms • **Max**: 60 ms	Yes	Yes

For telemetry-based collection, it is recommended to use the destination settings of **Batch size** as 16,384 bytes and **linger** as 500 ms, for optimal results.

Step 4 (Optional) To configure custom values that are different from global properties for a Kafka destination, in the **Customize Collector Settings** pane:

a) Select a **Collector**.

b) Enter values for the following fields:

- **Custom Buffer Memory**

- **Custom Batch Size**

> **Note** The **Custom Batch Size** cannot exceed the value of the **Custom Buffer Memory** at run time. In case, you do not provide a value in the **Custom Buffer Memory** field, the **Custom Batch Size** will be validated against the value in the **Buffer Memory** field.

- **Custom Linger**

- **Custom Request Timeout**

Figure 19: Add Destination Window

c) Click **+ Add Another** to repeat this step and add custom settings for another collector.

Note   Properties entered here for individual collectors take precedence over the global settings entered in Step 3. If you do not enter values in any field here, the values for the same will be taken from the Global properties entered in Step 3.

Step 5   Select a TCP/IP stack from the **Connection Details** options. The supported protocols are IPv4, IPv6, and FQDN.

Note   The FQDN addresses are supported only for the Kafka destinations.

Step 6   Complete the **Connection Details** fields as described in the following table. The fields displayed vary with the connectivity type you chose. The values you enter must match the values configured on the external Kafka or gRPC server.

Connectivity Type	Fields	Available in gRPC	Available in Kafka
IPv4	Enter the required **IPv4 Address/ Subnet Mask**, and **Port**. You can add multiple IPv4 addresses by clicking **+ Add Another** IPv4 subnet mask ranges from 1 to 32 and port range from 1024 to 65535.	Yes	Yes
IPv6	Enter the required **IPv6 Address/ Subnet Mask**, and **Port**. You can add multiple IPv6 addresses by clicking **+ Add Another**. IPv6 subnet mask ranges from 1 to 128 and port range from 1024 to 65535.	Yes	Yes
FQDN	Enter the required **Host Name**, **Domain Name**, and **Port**. The supported port range is from 1024 to 65535. You can add multiple FQDN addresses by clicking **+ Add Another**.	Yes	Yes

Step 7   (Optional) To connect securely to the Kafka or gRPC-based data destination, enable the **Enable Secure Communication** option by moving the slider under **Security Details**.

Step 8   For Kafka or gRPC-based data destinations, select the type of authentication process by choosing one of the following:

- **Mutual-Auth**: Authenticates external server and the Crosswork Data Gateway collector after the CA certificate, and Intermediate certificate or Key is uploaded to the Crosswork UI.

- **Server-Auth**: Authenticates external server and the Crosswork Data Gateway collector after the CA certificate is uploaded to the Crosswork UI. **Server-Auth** is the default authentication process.

Note   The authentication options are available only when **Enable Secure Communication** is enabled.

Step 9   Click **Save**.

What to do next

If you have enabled the **Enable Secure Communication** option, navigate to the **Certificate Management** page in the Cisco Crosswork UI (**Administration > Certificate Management**) and add the relevant certificate for the newly added data destination. This step is mandatory to establish a secure communication to the device. See Manage Certificates for more information.

Note   If you do not add the certificate or the certificate is incomplete for the data destination after enabling the **Enable Secure Communication** option, Cisco Crosswork sets the destination to an error state.

Delete a Data Destination

Follow the steps to delete a data destination:

Before you begin

A data destination can only be deleted if it is not associated with any collection job. We recommend to check in the **Collection Jobs** view to see if any collection jobs are using the data destination.

Step 1   From the main menu, choose **Administration** > **Data Gateway Global Settings** > **Data Destinations**.

Step 2   Select the Data destination(s) you want to delete from the list of destinations that is displayed and click 🗑 button.

Step 3   In **Delete Data Destination(s)** pop up, click **Delete** to confirm.

Manage Device Packages

Device management enables Crosswork Data Gateway to extend the data collection capabilities to the Cisco applications and third-party devices through the device packages. Crosswork Data Gateway supports system and custom device packages.

The system device and MIB packages are bundled in the Crosswork software and are automatically downloaded to the system instances. You cannot modify the system device and MIB packages.

Custom device package extends device coverage and collection capabilities to third-party devices.

The **Packages** pane can be accessed via **Administration** > **Data Gateway Global Settings** > **Packages**.

Custom Package

You can upload three types of custom packages to Cisco Crosswork:

1. **CLI Device Package**: To use CLI-based KPIs to monitor device health for third-party devices. All custom CLI device packages along with their corresponding YANG models should be included in file `custom-cli-device-packages.tar.xz`. Multiple files are not supported.

2. **Custom MIB Packages**: Custom MIBs and device packages can be specific to third-party devices or be used to filter the collected data or format it differently for Cisco devices. These packages can be edited. All custom SNMP MIB packages along with YANG models should be included in file `custom-mib-packages.tar.xz`. Multiple files are not supported.

> ✎
>
> **Note**   Cisco Crosswork Data Gateway enables SNMP polling on third-party devices for standard MIBs already included in the system. Proprietary MIBs are required only if the collection request references MIB TABLE names or SCALAR names from a proprietary MIB. However, if the requests are OID-based, then MIBs are not required.

3. **SNMP Device Package**: Cisco Crosswork Data Gateway allows you to extend the SNMP coverage by uploading custom SNMP device packages with any additional MIB and YANG descriptions you require.

Add Custom Packages

This is a list of guidelines about uploading packages to Cisco Crosswork.

1. You can upload one or more xar files in a single package tar.gz file.

2. Cisco Crosswork doesn't allow Custom MIB package files to overwrite the System MIB Package files. It results in a failed upload attempt.

3. Ensure that the custom package TAR file has just the package folders and none of the parent folder or hierarchy of folders as part of the TAR file. If not imported properly, Cisco Crosswork throws exceptions when executing the job with custom package.

> ✎
>
> **Note**   Cisco Crosswork does not validate the files being uploaded other than checking the file extension.

Follow these steps to upload a custom software package:

Before you begin

When uploading new MIBs as a part of Custom MIB Package, ensure that those new MIBs files can be uploaded within collectors along with existing System MIB files i.e., all dependencies in the files are resolved properly.

Note Performance of collection jobs executing the custom packages depends on how optimized the custom packages are. Ensure that you validate that the packages are optimized for the scale you want to deploy them for before uploading to Cisco Crosswork.

For information on how to validate custom MIBs and YANGs that is, to check if they can be uploaded to Cisco Crosswork, see Use Custom MIBs and Yangs on Cisco DevNet.

Step 1 From the main menu, choose **Administration** > **Data Gateway Global Settings**.

Step 2 In the **Custom Packages** pane, click ⊞.

To update the existing Custom CLI Device Package, click the upload icon next to the File name in the table.

Step 3 In the **Add Custom Packages** window that appears, select the type of package you want to import from the **Type** drop-down.

Step 4 Click in the blank field of **File Name** to open the file browser window and select the package to import and click **Open**.

Step 5 Add a description of the package in the **Notes** field. This is recommended if you have many packages, to be able to distinguish among them.

Step 6 Click **Upload**.

What to do next

Restart all impacted services to get the latest custom MIB package updates.

Delete Custom Package

Deleting a custom package causes deletion of all YANG and XAR files from Cisco Crosswork. This impacts all collection jobs using the custom package.

Follow the steps to delete a custom package:

Step 1 From the main menu, choose **Administration** > **Data Gateway Global Settings** > **Packages** > **Custom**.

Step 2 From the list displayed in the **Custom Packages** pane, select the package you want to delete and click 🗑.

Step 3 In the **Delete Custom Package** window that appears, click **Delete** to confirm.

System Device Package

A system device package contains one or more separate installable. Each file set in a package belongs to the same application.

The system device packages are supplied through the application-specific manifest file as a simple JSON file. System device packages are added or updated whenever the applications are installed or updated. Applications can install multiple device packages.

☞

Important	Administrators cannot modify the system device packages. Only applications can modify these files. To modify the system device packages, contact the Cisco Customer Experience team.

Figure 20: System Device Packages Window

To download a device package, click on the ⬇ button next to its name in the **File Name** column.

Configure Crosswork Data Gateway Global Parameters

Crosswork Data Gateway allows you to update the following parameters across all Crosswork Data Gateways in the network.

Note	These settings can only be accessed by an admin user.

Step 1   Navigate to **Administration** > **Data Gateway Global Settings** > **Data Gateway** > **Global Parameters**.

Figure 21: Global Parameters Window

Step 2   Change one of more of the following parameters.

Note	Ensure that the port values that you wish to update with are valid ports and do not conflict with the existing port values. Same port values must be configured on the device.

Parameter Name	Description
Number of CLI sessions	Maximum number of CLI sessions between a Crosswork Data Gateway and devices. The default value is 3. **Note** This value overrides any internal configuration set for the same parameter.
SNMP Trap Port	Default value is 1062.
Syslog UDP Port	Default value is 9514.
Syslog TCP Port	Default value is 9898.
Syslog TLS Port	Default value is 6514.
Force Re-Sync USM Engine Details for SNMPV3	USM details change whenever a device is rebooted or reimaged. SNMPV3 collections stop working whenever there is a change in any of the USM details. Enable this option to sync the USM details automatically whenever there is a change, after the very first collection failure. The default value is False.

Step 3 If you are updating ports, select **Yes** in the **Global Parameters** window that appears to confirm that collectors can be restarted. Updating ports causes the collectors to restart and pause any collection jobs that are running. The jobs resume automatically once the restart is complete.

Step 4 Click **Save** to apply your changes.

A window appears indicating if the parameters update on Crosswork Data Gateways in the network was successful or not.

1. If all the Crosswork Data Gateways were updated successfully, a success message appears in the UI indicating that the update was successful.

2. If any of the Crosswork Data Gateways in the network could not be updated, an Error window appears in the UI. Crosswork Data Gateway will automatically try to update the parameters on the failed Crosswork Data Gateway during recovery. Some of the collectors might be restarted as part of recovery.

Note One of the reasons the global parameters fail to update on a Crosswork Data Gateway could be that the OAM channel is down. After the OAM channel is reestablished, Crosswork Data Gateway tries sending these parameters to the Crosswork Data Gateway again (that is not in sync) and updates the values after comparison with the existing values.

What to do next

If you have updated any of the ports, navigate to **Administration** > **Data Gateway Management** > **Data Gateways** tab and verify that all Crosswork Data Gateways have the **Operational State** as **Up**.

Allocate Crosswork Data Gateway Resources

Crosswork Data Gateway allows you to dynamically configure and allocate memory at run time for collector services. You can allocate more memory to a heavily used collector or adjust the balance of resources from the UI.

Note   These settings can only be accessed by an admin user.

Memory and CPU sets that are currently configured for collector services are displayed in this page. Any changes that you make to the memory values in this page will apply to currently enrolled and future Crosswork Data Gateways.

Note   The list of collectors that is displayed in this page is dynamic, that is, it is specific to the deployment.

To update resource allocation for collectors:

Note   We recommend that you do not modify to these settings unless you are working with the Cisco Customer Experience (CX) team.

Step 1   The list of collectors and the resources consumed by each of them is displayed here.

Figure 22: Resource Window

Note   The NETCONF data collection support is deprecated starting from the CNC 5.0 release.

Step 2   Enter the updated values in the **Memory** field for the collectors for which you wish to change the memory allocation.

Attention   We recommend a minimum memory size of 2000 MB for the CLI and SNMP collector and 1000 MB for the NETCONF collectors.

Step 3   Drag the **Enable Collector** slider to On position to enable the data collection.

Step 4   Click **Save** once you are finished making the changes.

Updating the values for a collector causes the collector to restart and pause any collection jobs that are running. The jobs resume automatically once the restart is complete.

Enable or Disable Collectors

Crosswork Data Gateway starts collecting data through the configured collector after you enable data collection and continues until you disable it. You may disable a collector service to optimize the resources or when there is an issue with the collector affecting the data collection.

To enable or disable the collectors:

Before you begin

Review the following information before enabling or disabling a collector:

- The data collection for the SNMP and CLI collectors (containers) cannot be disabled. These collectors are required to check the device reachability.

- By default, the collectors are in the enabled state.

⚠️

Attention   Collectors should be disabled only during Day 0 or Day 1 configuration. If you plan on disabling a collector post Day 1, the administrator must manually clear the associated collection jobs.

Step 1   Navigate to **Administration > Data Gateway Global Settings > Data Gateway > Resource**.

The list of collectors and the resource limits is displayed.

Figure 23: Enabling or Disabling Collectors

Note	The NETCONF data collection support is deprecated starting from the CNC 5.0 release.

Step 2 Drag the **Enable/Disable Collectors** slider to On position to enable the collectors. A confirmation dialog box indicating that the enabling or disabling causes the collector to restart appears.

Step 3 Click **Yes**.

Step 4 Click **Save** to apply your changes.

After enabling data collection, you can set the memory utilization for the collector services. For more information on resource allocation, see Allocate Crosswork Data Gateway Resources.

Manage Crosswork Data Gateway Collection Jobs

A collection job is a task that Cisco Crosswork Data Gateway is expected to perform. Applications request data collection via collection jobs. Cisco Crosswork then assigns these collection jobs to a Cisco Crosswork Data Gateway to serve the request.

Crosswork Data Gateway supports multiple data collection protocols including CLI, MDT, SNMP, gNMI (dial-in), syslog, and NETCONF.

Note	The NETCONF data collection support is deprecated starting from the CNC 5.0 release.

Crosswork Data Gateway can collect any type of data as long as it can be forwarded over one of the supported protocols.

There are two types of data collection requests in Cisco Crosswork:

1. Data collection request to forward data for internal processes within Cisco Crosswork. Cisco Crosswork creates system jobs for this purpose. You cannot create or edit system jobs.

2. Data collection request to forward data to external data destinations. For more information on configuring the external data destinations (Kafka or gRPC), see Create and Manage External Data Destinations, on page 26.

You can forward collected data to an external data destination and Cisco Crosswork Health Insights in a single collection request by adding the external data destination when creating a KPI profile. For more information, see Section: *Create a New KPI Profile* in the *Cisco Crosswork Change Automation and Health Insights 4.3 User Guide.*

Note	1. Cisco Crosswork Data Gateway drops incoming traffic if there is no corresponding (listening) collection job request for the same. It also drops data, syslog events, and SNMP traps received from an unsolicited device (that is, not attached to Crosswork Data Gateway).
	2. Polled data cannot be requested from the device until Cisco Crosswork Data Gateway is ready to process and transmit the data.

You can view collection jobs currently active on all the Crosswork Data Gateway instances enrolled with Cisco Crosswork from the **Collection Jobs** page.

In the Cisco Crosswork UI, from the left navigation bar, choose **Administration** > **Collection Jobs**.

The left pane in the **Collection Jobs** page has two tabs, **Bulk Jobs** and **Parametrized Jobs**. **Bulk Jobs** list all the collection jobs that are created by the system, or from the UI and API here. The **Parametrized Jobs** pane lists all active jobs that are created by the Cisco Crosswork Service Health application.

Note   The **Parametrized Jobs** pane has no data and remains empty if Cisco Crosswork Service Health has not been deployed.

For more information, see Monitor Collection Jobs, on page 75.

Types of Collection Jobs

You can create the following list of collection jobs from the Cisco Crosswork UI (CLI) or using APIs to request data.

Note   The SNMP OID-based collection jobs can be created from the Cisco Crosswork UI or using the API, and SNMP-traps using the API.

- CLI Collection Job, on page 41
- SNMP Collection Job, on page 42
- MDT Collection Job, on page 49
- Syslog Collection Job, on page 51
- gNMI Collection Job, on page 60

For each collection job that you create, Cisco Crosswork Data Gateway executes the collection request and forwards the collected data to the preferred data destination.

This chapter describes how to create collection jobs from the Cisco Crosswork UI. To create collection jobs using APIs, see Crosswork Data Gateway APIs on Cisco Devnet.

The initial status for all the collection jobs in the Cisco Crosswork UI is Unknown. Upon receiving a collection job, Cisco Crosswork Data Gateway performs basic validations on it. If the collection job is valid, its status changes to **Successful**, else it changes to **Failed**.

The value of **Cadence** is in seconds. This value can be set between 10 seconds and 2764800 seconds (i.e. at most 32 days) max, depending on how frequently configured sensor data should be collected.

Note   We recommend a cadence of 60 seconds.

When collection from a device is skipped due to previous execution still in progress, Cisco Crosswork Data Gateway raises a warning log. No alert is generated for this scenario.

CLI Collection Job

Cisco Crosswork Data Gateway supports CLI-based data collection from the network devices. Following commands are supported for this type of collection job:

- `show` and the short version `sh`

- `traceroute`

- `dir`

Devices should not have any banner configuration for CLI collection to work properly. Please refer to device documentation on how to turn this off.

You can create a CLI collection job from the Cisco Crosswork UI or using APIs. See Cisco DevNet for more information.

Following is a sample payload of CLI collection job for a Kafka external destination. In this example, take note of two values in particular.

1. The device is identified with a UUID rather than an IP address.

2. The destination is also referenced by a UUID. For collections jobs built using the UI, Cisco Crosswork looks up the UUIDs. When you create your own collection jobs, you will need to look up these values.

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "CLI_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "658adb03-cc61-448d-972f-4fcec32cbfe8"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "cli_sensor": {
            "command": "show platform"
          }
        },
        "cadence_in_millisec": "tel:60000"
      }
    ],
    "sensor_output_configs": [
     {
        "sensor_data": {
          "cli_sensor": {
            "command": "show platform"
          }
        },
        "destination": {
```

```
            "destination_id": "1e71f2fb-ea65-4242-8efa-e33cec71b369",
            "context_id": "topic1"
        }
      }
    ]
  }
}
```

SNMP Collection Job

Cisco Crosswork Data Gateway supports SNMP-based data collection based on the OIDs supported on the devices.

The SNMP collector makes a poll request to Cisco Crosswork to get its configuration profile (a list of MIB objects to collect and a list of devices to fetch from). It determines the corresponding OIDs by looking up the prepackaged list of MIB modules or the custom list of MIB modules.

Note Cisco Crosswork Data Gateway enables SNMP polling on third-party devices for standard MIBs already included in the system. Proprietary MIBs are required only if the collection request references MIB TABLE names or SCALAR names from a proprietary MIB. However, if the requests are OID-based, then MIBs are not required.

After the OIDs are resolved, they are provided as input to the SNMP collectors.

The device packages can be imported into the Crosswork Data Gateway instance as described in Section Add Custom Packages, on page 33.

Supported SNMP versions for data polling and traps are:

- Polling Data

  - SNMP V2

  - SNMP V3 (no auth nopriv, auth no priv, authpriv)

  - Supported auth protocols – SHA-1, MD5

  - Supported priv protocols – AES-128, AES-192, AES-256, CiscoAES192, CiscoAES256, DES, and 3-DES.

- Traps

  - SNMP V2

  - SNMP V3 (no auth nopriv, auth no priv, authpriv)

Sample Configurations on Device:

The following table lists sample commands to enable various SNMP functions. For more information, refer to the platform-specific documentation.

Table 3: Sample configuration to enable SNMP on device

Version	Command	To...

V2c	`snmp-server group <group_name> v2c`
	
	`snmp-server user <user_name> <group_name> v2c`
		Define the SNMP version, user/user group details.

	`snmp-server host <host_ip> traps SNMP version <community_string> udp-port 1062`
	
	`snmp-server host a.b.c.d traps version 2c v2test udp-port 1062`
		Define the destination to which trap data must be forwarded.
		
		Note The IP address mentioned here must be the virtual IP address of the Crosswork Data Gateway.

	`snmp-server traps snmp linkup`
	
	`snmp-server traps snmp linkdown`
		Enable traps to notify link status.

Version	Command	To...
V3 **Note** Password for a SNMPv3 user must be at least 8 bytes.	`snmp-server host <host_IP> traps version 3 priv <user_name> udp-port 1062`	Define the destination to which trap data must be forwarded. **Note** The IP address mentioned here must be the virtual IP address of the Crosswork Data Gateway.
	`snmp-server user <user_name> <group_name> v3 auth md5 <password> priv aes 128 <password>`	Configures the SNMP server group to enable authentication for members of a specified named access list.
	`snmp-server view <user_name> < MIB > included`	Define what must be reported.
	`snmp-server group <group_name> v3 auth notify <user_name> read <user_name> write <user_name>`	Define the SNMP version, user/user group details.
	`snmp-server enable traps snmp [authentication ] [linkup ] [linkdown ] [warmstart ] [coldstart ]`	• When used without any of the optional keywords, enables authenticationFailure, linkUp, linkDown, warmStart, and coldStart traps. • When used with keywords, enables only the trap types specified. For example, to globally enable only linkUp and linkDown SNMP traps for all interfaces, use the **snmp-server enable traps snmp linkup linkdown** form of this command.

The SNMP Collector supports the following operations:

- SCALAR

Note   If a single collection requests for multiple scalar OIDs, you can pack multiple SNMP GET requests in a single `getbulkrequestquery` to the device.

- TABLE

- WALK

- COLUMN

These operations are defined in the sensor config (see payload sample below).

Note There is an optional **deviceParams** attribute **snmpRequestTimeoutMillis** (not shown in the sample payloads) that should be used if the device response time is more than 1500 milliseconds. It's not recommended to use **snmpRequestTimeoutMillis** unless you are certain that your device response time is high.

The value for snmpRequestTimeoutMillis should be specified in milliseconds:

The default and minimum value is 1500 milliseconds. However, there is no limitation on the maximum value of this attribute.

Following is an SNMP collection job sample:

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "SNMP_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "c70fc034-0cbd-443f-ad3d-a30d4319f937",
            "8627c130-9127-4ed7-ace5-93d3b4321d5e",
            "c0067069-c8f6-4183-9e67-1f2e9bf56f58"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.1.3.0",
              "snmp_operation": "SCALAR"
            }
          }
        },
        "cadence_in_millisec": "60000"
      },
      {
        "sensor_data": {
          "snmp_sensor": {
            "snmp_mib": {
              "oid": "1.3.6.1.2.1.31.1.1",
              "snmp_operation": "TABLE"
            }
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
```

```
"sensor_output_configs": [
  {
    "sensor_data": {
      "snmp_sensor": {
        "snmp_mib": {
          "oid": "1.3.6.1.2.1.1.3.0",
          "snmp_operation": "SCALAR"
        }
      }
    },
    "destination": {
      "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
      "context_id": "topic1_461cb8aa-a16a-44b8-b79f-c3daf3ea925f"
    }
  },
  {
    "sensor_data": {
      "snmp_sensor": {
        "snmp_mib": {
          "oid": "1.3.6.1.2.1.31.1.1",
          "snmp_operation": "TABLE"
        }
      }
    },
    "destination": {
      "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
      "context_id": "topic2_e7ed6300-fc8c-47ee-8445-70e543057f8a"
    }
  }
]
  }
}
```

SNMP Traps Collection Job

SNMP Traps Collection jobs can be created only via API. Trap listeners listen on a port and dispatch data to recipients (based on their topic of interest).

☞

Important Before starting the SNMP trap collection, install the Common EMS Services application and configure the host information for SNMP.

Crosswork Data Gateway listens on UDP port 1062 for Traps.

✎

Note Before submitting SNMP Trap collection jobs, SNMP TRAPS must be properly configured on the device to be sent to virtual IP address of the Crosswork Data Gateway.

SNMP Trap Collection Job Workflow

On receiving an SNMP trap, Cisco Crosswork Data Gateway:

1. Checks if any collection job is created for the device.

2. Checks the trap version and community string.

> ✎
>
> **Note** To prevent Crosswork Data Gateway from checking the community string for SNMP traps, select the **SNMP Disable Trap Check** check box when adding a device through the Crosswork UI. For more information about this option, see Add Devices through the UI.

3. For SNMP v3, also validates for user auth and priv protocol and credentials.

> ✎
>
> **Note** SNMPV3 auth-priv traps are dependent on the engineId of the device or router to maintain local USM user tables. Therefore, there will be an interruption in receiving traps whenever the engineId of the device or router changes. Please detach and attach the respective device to start receiving traps again.

Crosswork Data Gateway filters the traps based on the trap OID mentioned in the sensor path and sends only those requested.

If the collection job is invalid, there is missing configuration on the device, or no trap is received, the status of the job remains "Unknown". For list of supported Traps and MIBs, see List of Pre-loaded Traps and MIBs for SNMP Collection.

Crosswork Data Gateway supports three types of non-yang/OID based traps:

Table 4: List of Supported Non-Yang/OID based Traps

sensor path	purpose
*	To get all the traps pushed from the device without any filter.
MIB level traps	OID of one MIB notification (Ex: 1.3.6.1.2.1.138.0 to get all the isis-mib level traps)
Specific trap	OID of the specific trap (Ex: 1.3.6.1.6.3.1.1.5.4 to get the linkUp trap)

Following is an SNMP-Trap collection job sample:

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "TRAP_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "a9b8f43d-130b-4866-a26a-4d0f9e07562a",
            "8c4431a0-f21d-452d-95a8-84323a19e0d6",
            "eaab2647-2351-40ae-bf94-6e4a3d79af3a"
          ]
        }
```

```
        }
      },
      "sensor_input_configs": [
        {
          "sensor_data": {
            "trap_sensor": {
              "path": "1.3.6.1.6.3.1.1.4"
            }
          },
          "cadence_in_millisec": "60000"
        }
      ],
      "sensor_output_configs": [
        {
          "sensor_data": {
            "trap_sensor": {
              "path": "1.3.6.1.6.3.1.1.4"
            }
          },
          "destination": {
            "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
            "context_id": "topic1_696600ae-80ee-4a02-96cb-3a01a2415324"
          }
        }
      ]
    }
  }
}
```

Enabling Traps forwarding to external applications

We recommended selectively enabling only those traps that are needed by Crosswork on the device.

To identify the type of trap from the data received on the destination, look for *oid* (OBJECT_IDENTIFIER, for example, `1.3.6.1.6.3.1.1.4.1.0`) and *strValue* associated to the *oid* in the OidRecords (application can match the OID of interest to determine the kind of trap).

Following are the sample values and a sample payload to forward traps to external applications:

- Link up

  `1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4`

- Link Down

  `1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3`

- Syslog

  `1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.9.9.41.2.0.1`

- Cold Start

  `1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1`

```
{
  "nodeIdStr": "BF5-XRV9K1.tr3.es",
  "nodeIdUuid": "C9tZ5lJoSJKf5OZ67+U5JQ==",
  "collectionId": "133",
  "collectionStartTime": "1580931985267",
  "msgTimestamp": "1580931985267",
  "dataGpbkv": [
    {
      "timestamp": "1580931985267",
      "name": "trapsensor.path",
```

```
        "snmpTrap": {
          "version": "V2c",
          "pduType": "TRAP",
          "v2v3Data": {
            "agentAddress": "172.70.39.227",
            "oidRecords": [
              {
                "oid": "1.3.6.1.2.1.1.3.0",
                "strValue": "7 days, 2:15:17.02"
              },
              {
                "oid": "1.3.6.1.6.3.1.1.4.1.0",  // This oid is the Object Identifier.
                "strValue": "1.3.6.1.6.3.1.1.5.3" // This is the value that determines the
kind of trap.
              },
              {
                "oid": "1.3.6.1.2.1.2.2.1.1.8",
                "strValue": "8"
              },
              {
                "oid": "1.3.6.1.2.1.2.2.1.2.8",
                "strValue": "GigabitEthernet0/0/0/2"
              },
              {
                "oid": "1.3.6.1.2.1.2.2.1.3.8",
                "strValue": "6"
              },
              {
                "oid": "1.3.6.1.4.1.9.9.276.1.1.2.1.3.8",
                "strValue": "down"
              }
            ]
          }
        }
      }
    }
  ],
  "collectionEndTime": "1580931985267",
  "collectorUuid": "YmNjZjEzMTktZjlOS00NTE5LWI4OTgtY2Y1ZmQxZDFjNWExOlRSQVBfQ09MTEVDVDE9S",
  "status": {
    "status": "SUCCESS"
  },
  "modelData": {},
  "sensorData": {
    "trapSensor": {
      "path": "1.3.6.1.6.3.1.1.5.4"
    }
  },
  "applicationContexts": [
    {
      "applicationId": "APP1",
      "contextId": "collection-job-snmp-traps"
    }
  ]
}
```

MDT Collection Job

Crosswork Data Gateway supports data collection from network devices using Model-driven Telemetry (MDT) to consume telemetry streams directly from devices (for IOS-XR based platforms only).

Crosswork Data Gateway supports data collection for the following transport mode:

   • MDT TCP Dial-out Mode

Cisco Crosswork leverages NSO to push the required MDT configuration to the devices and will send the corresponding collection job configuration to the Crosswork Data Gateway.

> **Note**
> - If there is some change (update) in existing MDT jobs between backup and restore operations, Cisco Crosswork does not replay the jobs for config update on the devices as this involves NSO. You have to restore configs on NSO/devices. Cisco Crosswork only restores the jobs in database.
> - Before using any YANG modules, check if they are supported. See Section: List of Pre-loaded YANG Modules for MDT Collection

Following is a sample of MDT collection payload:

```
{
 "collection_job": {
  "job_device_set": {
   "device_set": {
    "device_group": "mdt"
   }
  },
  "sensor_output_configs": [{
    "sensor_data": {
     "mdt_sensor": {
      "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"

     }
    },
    "destination": {
     "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
     "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
    }
   },
   {
    "sensor_data": {
     "mdt_sensor": {
     "path": "Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"

     }
    },
    "destination": {
     "context_id": "cw.mdt_sensor.cisco-ios-xr-infra-statsd-oper.gpb",
     "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
    }
   }
  ],
  "sensor_input_configs": [{
    "sensor_data": {
     "mdt_sensor": {
     "path": "Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/data-rate"

     }
    },
    "cadence_in_millisec": "70000"
   }, {
    "sensor_data": {
     "mdt_sensor": {
      "path":
"Cisco-IOS-XR-infra-statsd-oper:infra-statistics/interfaces/interface/latest/generic-counters"
```

```
     }
    },
    "cadence_in_millisec": "70000"
   }
  ],
  "application_context": {
   "context_id": "c4",
   "application_id": "a4-mdt"
  },
  "collection_mode": {
   "lifetime_type": "APPLICATION_MANAGED",
   "collector_type": "MDT_COLLECTOR"
  }
 }
}
```

MDT Collection Job Workflow

When an MDT based KPI is activated on a device, Cisco Crosswork

1. Sends a configuration request to NSO to enable the data collection on the target devices.

2. Send a collection job create request to the Crosswork Data Gateway.

3. Crosswork Data Gateway creates a distribution to send the data collected to the destination you specify.

Syslog Collection Job

Crosswork Data Gateway supports Syslog-based events collection from devices.

☞

Important Before starting the Syslog trap collection, install the Common EMS Services application and configure the host information for Syslog.

The following Syslog formats are supported:

- RFC5424 syslog format

- RFC3164 syslog format

✎

Note To gather Syslog data from Crosswork Data Gateway in the network, when adding a device, select the YANG_CLI capability and configure other parameters to receive Syslog data from Crosswork Data Gateway. Refer to the platform-specific documentation.

While the order of the configuration steps does not matter, you must complete both the steps, or no data will be sent or collected. For sample device configuration, see Configure Syslog (Non-Secure) on Device, on page 55. Cisco Crosswork also allows you to set up secure syslog communication to the device. For more information, see Configure Secure Syslog on Device, on page 56.

Following is a sample Syslog collection payload:

```
{
  "collection_job": {
      "job_device_set": {
      "device_set": {
        "devices": {
```

```
          "device_ids": [
            "c6f25a33-92e6-468a-ba0d-15490f1ce787"
          ]
        }
      }
    },
    "sensor_output_configs": [
      {
        "sensor_data": {
          "syslog_sensor": {
            "pris": {
                "facilities": [0, 1, 3, 23,4],
                "severities": [0, 4, 5, 6, 7]
            }
          }
        },
        "destination": {
          "context_id": "syslogtopic",
          "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
        }
      }
    ],
    "sensor_input_configs": [
      {
        "sensor_data": {
          "syslog_sensor": {
            "pris": {
                "facilities": [0,1, 3, 23,4],
                "severities": [0,4, 5, 6, 7]
            }
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "application_context": {
      "context_id": "demomilesstone2syslog",
      "application_id": "SyslogDemo2"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "SYSLOG_COLLECTOR"
    }
  }
}
```

- You can filter the output of syslog data collection by specifying either PRI-based SyslogSensor OR Filters-based SyslogSensor. Syslog events matching the facilities and severities mentioned in the payload are sent to the specified destination. All other nonmatching syslog events are dropped. You can specify the filter based on regEx, severity, or facility.

- If you have specified values for severity and facility, then both the conditions are combined based on the logical operator specified at Filters level.

- You can specify a maximum of three filters combinations using the logical operator AND or OR. By default, the AND operator is applied if do not specify an operator.

Syslog Collection Job Output

When you onboard a device from Cisco Crosswork UI (**Device Management > Network Devices > Device Details**), the value you choose in the **Syslog Format** field configures the format in which syslog events

received from the device should be parsed by the Syslog Collector. You can choose either **UNKNOWN**, **RFC5424** or **RFC3164**.

Following is the sample output for each of the options:

1. **UNKNOWN** - Syslog Collection Job output contains syslog events as received from device.

> **Note** If the device is configured to generate syslog events in RFC5424/RFC3164 format but no format is specified in the **Syslog Format** field, this is considered as **UNKNOWN** by default.

Sample output:

```
node_id_str: "xrv9k-VM8"
node_id_uuid: ":i\300\216>\366BM\262\270@\337\225\2723&"
collection_id: 1056
collection_start_time: 1616711596200
msg_timestamp: 1616711596201
data_gpbkv {
  timestamp: 1616711596201
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<6>1 Mar 25 15:34:41.321 PDT - SSHD_ 69570 - - 98949:
RP/0/RP0/CPU0:SSHD_[69570]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated
user \'admin\' from \'40.40.40.116\' on \'vty0\'(cipher \'aes128-ctr\', mac \'hmac-sha1\')
 \n"
  }
  fields {
    name: "DEVICE_IP"
    string_value: "40.40.40.30"
  }
}
collection_end_time: 1616711596200
collector_uuid: "17328736-b726-4fe3-b922-231a4a30a54f:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
model_data {
}
sensor_data {
  syslog_sensor {
    pris {
      facilities: 0
      facilities: 3
      facilities: 4
      facilities: 23
      severities: 0
      severities: 5
      severities: 6
      severities: 7
    }
  }
}
application_contexts {
  application_id: "SyslogApp-xr-8-job1"
  context_id: "xr-8-job1"
}
version: "1"
```

2. **RFC5424** - If the device is configured to generate syslog events in RFC5424 format and the RFC5424 format is selected in the **Syslog Format** field, the Syslog Job Collection output contains syslog events as received from device (RAW) and the RFC5424 best-effort parsed syslog events from the device.

Note The syslog collector will parse the syslog event on best efforts as per the following Java RegEx pattern:

RFC5424

"^<(?<pri>\\d+)>(?<version>\\d{1,3})\\s*(?<date>(([0-9]{4}\\s+)?[a-zA-Z]{3}\\s+\\d+\\s+\\d+:\\d+:\\d+.\\d{3}\\s+[a-zA-Z]{3}?[:]?)9T:.Z-]+))\\s*(?<host>\\S+)\\s*(?<processname>\\S+)\\s*(?<procid>\\S+)\\s*(?<msgid>\\S+)\\s*(?<structureddata>(-|\\[.+\\]))\\s<message>.+)$";

Sample output:

```
....
....


collection_start_time: 1596307542398
msg_timestamp: 1596307542405
data_gpbkv {
  timestamp: 1596307542405
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<13>1 2020 Aug  1 12:03:32.461 UTC:  iosxr254node config 65910 - -
2782: RP/0/RSP0/CPU0:2020 Aug  1 12:03:32.461 UTC: config[65910]: %MGBL-SYS-5-CONFIG_I
: Configured from console by admin on vty0 (10.24.88.215) \n"
  }
  fields {
    name: "RFC5424"
    string_value: "pri=13,  severity=5,  facility=1,  version=1,
date=2020-08-01T12:03:32.461,  remoteAddress=/172.28.122.254,  host=\'iosxr254node\',
message=\'2782: RP/0/RSP0/CPU0:2020 Aug  1 12:03:32.461 UTC: config[65910]:
%MGBL-SYS-5-CONFIG_I : Configured from console by admin on vty0 (10.24.88.215) \',
messageId=null, processName=config, structuredDataList=null"
  }
  fields {
    name: "DEVICE_IP"
    string_value: "172.28.122.254"
  }
}
collection_end_time: 1596307542404
collector_uuid: "ac961b09-8f67-4c93-a99a-31eef50f7fa9:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
...
...
```

3. **RFC3164** - If the device is configured to generate syslog events in RFC3164 format and the RFC3164 format is selected in **Syslog Format** field, the Syslog Job Collection output contains both RAW (as received from device) syslog events and the RFC3164 best-effort parsed syslog events from the device.

✎

Note   The syslog collector will parse the syslog event on best efforts as per the following Java RegEx pattern:

RFC3164

"^(<(?<pri>\\d+)>[:]*\\s*)?(?<date>(*[a-zA-Z]{3}\\s+\\d+\\s+[0-9]{4}\\s+\\d+:\\d+:\\d+\\.[\\d{3}\\s+]+[[a-zA-Z]{3}[:]*]?\\s+)|(([[a-zA-Z]{3}\\s+\\d+\\s+\\d+:\\d+:\\d+[.]*[\\d{3}\\s+]+[[a-zA-Z]{3}[:]*]*)|([0-9T:.Z-]+))\\s+(?<host>\\S+)?\\s+((?<tag>[^\\[\\s\\]]+ <procid>\\d+)\\])?:)*\\s*(?<message>.+)$";

Sample output:

```
....
.....
collection_id: 20
collection_start_time: 1596306752737
msg_timestamp: 1596306752743
data_gpbkv {
  timestamp: 1596306752743
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<14>2020 Aug  1 11:50:22.799 UTC:  iosxr254node 2756:
RP/0/RSP0/CPU0:2020 Aug  1 11:50:22.799 UTC: config[65910]: %MGBL-CONFIG-6-DB_COMMIT :
Configuration committed by user \'admin\'. Use \'show configuration commit changes
1000000580\' to view the changes. \n"
  }
  fields {
    name: "RFC3164"
    string_value: "pri=14,  severity=6,  facility=1,  version=null,
date=2020-08-01T11:50:22.799,  remoteAddress=/172.28.122.254,  host=\'iosxr254node\',
message=\'RP/0/RSP0/CPU0:2020 Aug  1 11:50:22.799 UTC: config[65910]:
%MGBL-CONFIG-6-DB_COMMIT : Configuration committed by user \'admin\'. Use \'show
configuration commit changes 1000000580\' to view the changes. \', tag=2756"
  }
  fields {
    name: "DEVICE_IP"
    string_value: "172.28.122.254"
  }
}
collection_end_time: 1596306752742
collector_uuid: "ac961b09-8f67-4c93-a99a-31eef50f7fa9:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
....
....
```

If the Syslog Collector is unable to parse the syslog events according to the format specified in the **Syslog Format** field, then the Syslog Collection Job output contains syslog events as received from device (RAW).

Configure Syslog (Non-Secure) on Device

This section lists sample configuration to configure syslog in the RFC3164 or RFC5424 format on the device.

Configure RFC3164 Syslog format

Note The configuration highlighted in the code below is required to avoid formatting issues in the parsed output.

For Cisco IOS XR devices:

```
logging <CDG IP> port 9514 OR logging <CDG IP> vrf <vrfname> port 9514
logging trap [severity]
logging facility [facility value]
logging suppress duplicates
service timestamps log datetime msec show-timezone year
logging hostnameprefix <some host related prefix e.g.iosxrhost2>
```

For Cisco IOS XE Devices:

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host <CDG IP> transport tcp port 9898 session-id string <sessionidstring> --> To
use TCP channel
OR
logging host <CDG IP> transport udp port 9514 session-id string <sessionidstring> ---> To
use UDP channel
OR
logging host <CDG IP> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
```

Configure RFC5424 Syslog format

For Cisco IOS XR devices:

```
logging <CDG IP> port 9514 OR logging <server 1> vrf <vrfname> port 9514
logging trap [severity]
logging facility [facility value]
logging suppress duplicates
service timestamps log datetime msec show-timezone year
logging hostnameprefix <some host related prefix e.g.iosxrhost2>
logging format rfc5424
```

For Cisco IOS XE Devices:

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host <CDG IP> transport tcp port 9898 session-id string <sessionidstring> --> To
use TCP channel
OR
logging host <CDG IP> transport udp port 9514 session-id string <sessionidstring> ---> To
use UDP channel
OR
logging host <CDG IP> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
logging trap syslog-format 5424 --> if applicable
```

Configure Secure Syslog on Device

Follow these steps to establish a secure syslog communication to the device.

1. Download the Cisco Crosswork trust chain from the **Certificate Management UI** page in Cisco Crosswork.

2. Configure the device with the Cisco Crosswork trust chain.

Download Syslog Certificates

1. In the Cisco Crosswork UI, go to **Administration > Certificate Management**.

2. Click *i* in the '**crosswork-device-syslog**' row.

3. Click **Export All** to download the certificates.

   The following files are downloaded to your system.

Name
🔒 interrmediate.key
interrmediate.crt
ca.crt

Configure Cisco Crosswork Trustpoint on Device

Sample XR Device Configuration to enable TLS

```
RP/0/RSP0/CPU0:ASR9k(config)#crypto ca trustpoint syslog-root
RP/0/RSP0/CPU0:ASR9k(config-trustp)#enrollment terminal
RP/0/RSP0/CPU0:ASR9k(config-trustp)#crl optional
RP/0/RSP0/CPU0:ASR9k(config-trustp)#commit
RP/0/RSP0/CPU0:ASR9k(config-trustp)#end
RP/0/RSP0/CPU0:ASR9k#
RP/0/RSP0/CPU0:ASR9k#crypto ca authenticate syslog-root
Fri Jan 22 11:07:41.880 GMT


Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIGKzCCBBOgAwIBAgIRAKfyU89yjmrXVDRKBWuSGPgwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
.............................................................
.............................................................
jPQ/UrO8N3sC1gGJX7CIIh5cE+KIJ51ep8i1eKSJ5wHWRTmv342MnG2StgOTtaFF
vrkWHD02o6jRuYXDWEUptDOg8oEritZb+SNPXWUc/2mbYog6ks6EeMC69VjkZPo=
-----END CERTIFICATE-----

Read 1583 bytes as CA certificate
  Serial Number  : A7:F2:53:CF:72:8E:6A:D7:54:34:4A:05:6B:92:18:F8
  Subject:
              CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
              CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:09 UTC Sat Jan 16 2021
  Validity End   : 02:37:09 UTC Thu Jan 15 2026
  SHA1 Fingerprint:
              209B3815271C22ADF78CB906F6A32DD9D97BBDBA

Fingerprint: 2FF85849EBAAB9B059ACB9F5363D5C9CDo you accept this certificate? [yes/no]: yes
RP/0/RSP0/CPU0:ASR9k#config
RP/0/RSP0/CPU0:ASR9k(config)#crypto ca trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-trustp)#enrollment terminal
RP/0/RSP0/CPU0:ASR9k(config-trustp)#crl optional
RP/0/RSP0/CPU0:ASR9k(config-trustp)#commit
RP/0/RSP0/CPU0:ASR9k#crypto ca authenticate syslog-inter
Fri Jan 22 11:10:30.090 GMT
```

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIGFDCCA/ygAwIBAgIRAkhqHQXcJzQzeQK6U2wn8PIwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
...............................................................
...............................................................
5lBk617z6cxFER5c+/PmJFhcreisTxXg1aJbFdnB5C8f+0uUIdLghykQ/zaZGuBn
AAB70c9r9OeKGJWzvv1e2U8HH1pdQ/nd
-----END CERTIFICATE-----

Read 1560 bytes as CA certificate
  Serial Number  : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
  Subject:
               CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
               CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:11 UTC Sat Jan 16 2021
  Validity End   : 02:37:11 UTC Mon Jan 16 2023
  SHA1 Fingerprint:
               B06F2BFDE95413A8D08A01EE3511BC3D42F01E59

CA Certificate validated using issuer certificate.
RP/0/RSP0/CPU0:ASR9k#show crypto ca certificates
Fri Jan 22 15:45:17.196 GMT


Trustpoint      : syslog-root
====================================================
CA certificate
  Serial Number  : A7:F2:53:CF:72:8E:6A:D7:54:34:4A:05:6B:92:18:F8
  Subject:
      CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
      CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:09 UTC Sat Jan 16 2021
  Validity End   : 02:37:09 UTC Thu Jan 15 2026
  SHA1 Fingerprint:
      209B3815271C22ADF78CB906F6A32DD9D97BBDBA


Trustpoint      : syslog-inter
====================================================
CA certificate
  Serial Number  : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
  Subject:
      CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
      CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:11 UTC Sat Jan 16 2021
  Validity End   : 02:37:11 UTC Mon Jan 16 2023
  SHA1 Fingerprint:
      B06F2BFDE95413A8D08A01EE3511BC3D42F01E59
RP/0/RSP0/CPU0:ASR9k(config)#logging tls-server syslog-tb131
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#tls-hostname 10.13.0.159
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#severity debugging
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#vrf default
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#commit
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#exit
RP/0/RSP0/CPU0:ASR9k(config)#exit
RP/0/RSP0/CPU0:ASR9k#exit
```

```
RP/0/RSP0/CPU0:ASR9k#show running-config logging
Fri Jan 22 11:17:19.385 GMT
logging tls-server syslog-tb131
vrf default
severity debugging
trustpoint syslog-inter
tls-hostname <CDG Southbound IP>
!
logging trap debugging
logging format rfc5424
logging facility user
logging hostnameprefix ASR9k
logging suppress duplicates

RP/0/RSP0/CPU0:ASR9k#
```

Sample XE Device Configuration to enable TLS

```
csr8kv(config)#crypto pki trustpoint syslog-root
csr8kv(ca-trustpoint)#enrollment terminal
csr8kv(ca-trustpoint)#revocation-check none
csr8kv(ca-trustpoint)#chain-validation stop
csr8kv(ca-trustpoint)#end
csr8kv(config)#crypto pki authenticate syslog-root

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFPjCCAyYCCQCO6pK5AOGYdjANBgkqhkiG9w0BAQsFADBhMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCQ0ExETAPBgNVBAcMCE1pbHBpdGFzMQ4wDAYDVQQKDAVDaXNj
..............................................................
..............................................................
JbimOpXAncoBLo14DXOJLvMVRjn1EULE9AXXCNfnrnBx7jL4CV+qHgEtF6oqclFW
JEA=
-----END CERTIFICATE-----

Certificate has the following attributes:
      Fingerprint MD5: D88D6D8F E53750D4 B36EB498 0A435DA1
      Fingerprint SHA1: 649DE822 1C222C1F 5101BEB8 B29CDF12 5CEE463B

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported


csr8kv(config)#crypto pki trustpoint syslog-intermediate
csr8kv(ca-trustpoint)#enrollment terminal
csr8kv(ca-trustpoint)#revocation-check none
csr8kv(ca-trustpoint)#chain-validation continue syslog-root
csr8kv(ca-trustpoint)#end
csr8kv(config)#crypto pki authenticate syslog-intermediate

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFfTCCA2WgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVT
..............................................................
..............................................................
Nmz6NQynD7bxdQa9Xq9kyPuY3ZVKXkf312IRH0MEy2yFX/tAen9JqOeZ1g8canmw
TxsWA5TLzy1RmxqQh88f0CM=
-----END CERTIFICATE-----
Trustpoint 'syslog-intermediate' is a subordinate CA.
```

```
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
        Fingerprint MD5: FE27BDBE 9265208A 681670AC F59A2BF1
       Fingerprint SHA1: 03F513BD 4BEB689F A4F4E001 57EC210E 88C7BD19

csr8kv(config)#logging host <CDG Southbound IP> transport tls port 6514
csr8kv(config)#logging trap informational syslog-format rfc5424
csr8kv(config)#logging facility user
csr8kv(config)#service timestamps log datetime msec year show-timezone

csr8kv(config)#logging tls-profile tlsv12
```

Syslog configuration to support FQDN

Run the following commands in addition to the sample device configuration to enable TLS to support FQDN.

1. Configure the domain name and DNS IP has to be configured on the device.

```
RP/0/RSP0/CPU0:ASR9k#config
RP/0/RSP0/CPU0:ASR9k(config)#domain name <DNS domain name>
RP/0/RSP0/CPU0:ASR9k(config)#domain name-server <DNS server IP>
```

2. Configure Crosswork Data Gateway VIP FQDN for tls-hostname.

```
RP/0/RSP0/CPU0:ASR9k(config)#logging tls-server syslog-tb131
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#tls-hostname <CDG VIP FQDN>
```

gNMI Collection Job

Cisco Crosswork supports gRPC Network Management Interface (gNMI) based telemetry data collection via Cisco Crosswork Data Gateway. It supports only gNMI Dial-In (gRPC Dial-In) streaming telemetry data based on subscription and relaying subsequent subscription response (notifications) to the requested destinations.

> **Note** gNMI collection is supported as long as the models are supported by the target device platform. gNMI must be configured on devices before you can submit gNMI collection jobs. Check platform-specific documentation.

To configure gNMI on the device, see Enable gNMI on Device, on page 68.

In gNMI, both secure and insecure mode can co-exist on the device. Cisco Crosswork gives preference to secure mode over non-secure mode based on the information passed in the inventory.

If a device reloads, gNMI collector ensures that the existing subscriptions are re-subscribed to the device.

gNMI specification does not have a way to mark end of message. Hence, Destination and Dispatch cadence is not supported in gNMI collector.

Cisco Crosswork Data Gateway supports the following types of subscribe options for gNMI:

Table 5: gNMI Subscription Options

Type	Subtype	Description
Once		Collects and sends the current snapshot of the system configuration only once for all specified paths

Type	Subtype	Description
Stream	SAMPLE	Cadence-based collection.
	ON_CHANGE	First response includes the state of all the elements for the subscribed path, followed by subsequent updates to the changes leaf values.
	TARGET_DEFINED	Router/Device chooses the mode of subscription on a per-leaf basis based on the subscribed path (i.e. one of SAMPLE or ON_CHANGE)

Crosswork Data Gateway supports the ability to subscribe to multiple subscription paths in a single subscription list to the device. For example, you can specify a combination of ON_CHANGE and subscription mode ONCE collection jobs. ON_CHANGE mode collects data only on change of any particular element for the specified path, while subscription mode ONCE collects and sends current system data only once for the specified path.

Note
- Crosswork Data Gateway relies on the device to declare the support of one or more modes.

- gNMI sensor path with default values does not appear in the payload. This is a known protobuf behavior.

  For boolean the default value is false. For enum, it is gnmi.proto specified.

  Example 1:

```
message GNMIDeviceSetting {
bool suppress_redundant = 1;
bool allow_aggregation = 4;
bool updates_only = 6;
}
```

  Example 2:

```
enum SubscriptionMode {
TARGET_DEFINED = 0; //default value will not be printed
ON_CHANGE = 1;
SAMPLE = 2;
}
```

Following is a sample gNMI collection payload. In this sample you see two collections for the device group "milpitas". The first collects interface statistics, every 60 seconds using the "mode" = "SAMPLE". The second job captures any changes to the interface state (up/down). If this is detected it is simply sent "mode" = "STREAM" to the collector.

```
{
    "collection_job": {
        "job_device_set": {
            "device_set": {
                "device_group": "milpitas"
            }
        },
        "sensor_output_configs": [{
            "sensor_data": {
                "gnmi_standard_sensor": {
```

```
                         "Subscribe_request": {
                             "subscribe": {
                                 "subscription": [{
                                     "path": {
                                         "origin": "openconfig-interfaces",
                                         "elem": [{
                                             "name": "interfaces/interface/state/ifindex"
                                         }]
                                     },
                                     "mode": "SAMPLE",
                                     "sample_interval": 10000000000
                                 }, {
                                     "path": {
                                         "origin": "openconfig-interfaces",
                                         "elem": [{
                                             "name":
"interfaces/interfaces/state/counters/out-octets"
                                         }]
                                     },
                                     "mode": "ON_CHANGE",
                                     "sample_interval": 10000000000
                                 }],
                                 "mode": "STREAM",
                                 "encoding": "JSON"
                             }
                         }
                     }
                 },
                 "destination": {
                     "context_id": "hukarz",
                     "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
                 }
             }],
             "sensor_input_configs": [{
                 "sensor_data": {
                     "gnmi_standard_sensor": {
                         "Subscribe_request": {
                             "subscribe": {
                                 "subscription": [{
                                     "path": {
                                         "origin": "openconfig-interfaces",
                                         "elem": [{
                                             "name": "interfaces/interface/state/ifindex"
                                         }]
                                     },
                                     "mode": "SAMPLE",
                                     "sample_interval": 10000000000
                                 }, {
                                     "path": {
                                         "origin": "openconfig-interfaces",
                                         "elem": [{
                                             "name":
"interfaces/interfaces/state/counters/out-octets"
                                         }]
                                     },
                                     "mode": "ON_CHANGE",
                                     "sample_interval": 10000000000
                                 }],
                                 "mode": "STREAM",
                                 "encoding": "JSON"
                             }
                         }
                     }
                 },
```

```
            "cadence_in_millisec": "60000"
        }],
        "application_context": {
            "context_id": "testing.group.gnmi.subscription.onchange",
            "application_id": "testing.postman.gnmi.standard.persistent"
        },
        "collection_mode": {
            "lifetime_type": "APPLICATION_MANAGED",
            "collector_type": "GNMI_COLLECTOR"
        }
    }
}
```

Enable Secure gNMI communication between Device and Crosswork Data Gateway

Cisco Crosswork can only use one rootCA certificate (self-signed or signed by a trusted root CA) which means all device certificates must be signed by same CA.

If you have certificates signed by a different a trusted root CA, you can skip the first step and start from Step 2 to import the rootCA certificate in Cisco Crosswork.

Follow these steps to enable secure gNMI between Cisco Crosswork and the devices:

1. Generate the certificates. See Generate Device Certificates, on page 63.

2. Upload the certificates to the Crosswork Certificate Management UI in Cisco Crosswork. See Configure gNMI Certificate, on page 65.

3. Update device configuration with secure gNMI port details from Cisco Crosswork UI. See Update Protocol on Device from Cisco Crosswork, on page 67.

4. Enable gNMI on the device. See Enable gNMI on Device, on page 68.

5. Enable gNMI bundling on the device. See Configuring gNMI Bundling for IOS XR, on page 69.

6. Configure the certificates and device key on the device. See Import and Install Certificates on Devices, on page 66.

Generate Device Certificates

This section explains how to create certificates with OpenSSL.

Steps to generate certificates have been validated with Open SSL and Microsoft. For the purpose of these instructions, we have explained the steps to generate device certificates with Open SSL.

> **Note** To generate device certificates with a utility other than Open SSL or Microsoft, consult the Cisco Support Team.

1. **Create the rootCA certificate**

```
# openssl genrsa -out rootCA.key
# openssl req -subj /C=/ST=/L=/O=/CN=CrossworkCA -x509 -new -nodes -key rootCA.key -sha256
 -out rootCA.pem -days 1024
```

In the above command, the `days` attribute determines the how long the certificate is valid. The minimum value is 30 days which means you will need to update the certificates every 30 days. We recommend setting the value to 365 days.

2. **Create device key and certificate**

```
# openssl genrsa -out device.key
# openssl req -subj /C=/ST=/L=/O=/CN=Crosswork -new -key device.key -out device.csr
# openssl x509 -req -extfile <(printf "subjectAltName=IP.0: 10.58.56.18") -in device.csr
 -CA rootCA.pem -CAkey rootCA.key -CAcreateserial -sha256 -out device.crt -days 1024
```

If you have multiple devices, instead of creating multiple device certificates, you can specify multiple device IP addresses separated by a comma in the subjectAltName.

```
# openssl x509 -req -extfile <(printf "subjectAltName=IP.0: 10.58.56.18, IP.1:
10.58.56.19, IP.2: 10.58.56.20 ..... ") -in device.csr -CA rootCA.pem -CAkey rootCA.key
 -CAcreateserial -sha256 -out device.crt -days 1024
```

3. **Verify if the certificate is created and contains the expected SAN details**

```
# openssl x509 -in device.crt -text -noout
```

The following is a sample output:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            66:38:0c:59:36:59:da:8c:5f:82:3b:b8:a7:47:8f:b6:17:1f:6a:0f
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = rootCA
        Validity
            Not Before: Oct 28 17:44:28 2021 GMT
            Not After : Aug 17 17:44:28 2024 GMT
        Subject: CN = Crosswork
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c6:25:8a:e8:37:7f:8d:1a:7f:fa:e2:d6:10:0d:
                    b8:e6:2b:b0:b0:7e:ab:c9:f9:14:a3:4f:2e:e6:30:
                    97:f4:cd:d6:11:7d:c0:a6:9b:43:83:3e:26:0f:73:
                    42:89:3c:d7:62:7b:04:af:0b:16:67:4c:8e:60:05:
                    cc:dd:99:37:3f:a4:17:ed:ff:28:21:20:50:6f:d9:
                    be:23:78:07:dc:1e:31:5e:5f:ca:54:27:e0:64:80:
                    03:33:f1:cd:09:52:07:6f:13:81:1b:e1:77:e2:08:
                    9f:b4:c5:97:a3:71:e8:c4:c8:60:18:fc:f3:be:5f:
                    d5:37:c6:05:6e:9e:1f:65:5b:67:46:a6:d3:94:1f:
                    38:36:54:be:23:28:cc:7b:a1:86:ae:bd:0d:19:1e:
                    77:b7:bd:db:5a:43:1f:8b:06:4e:cd:89:88:e6:45:
                    0e:e3:17:b3:0d:ba:c8:25:9f:fc:40:08:87:32:26:
                    69:62:c9:57:72:8a:c2:a1:37:3f:9d:37:e9:69:33:
                    a5:68:0f:8f:f4:31:a8:bc:34:93:a3:81:b9:38:87:
                    2a:87:a3:4c:e0:d6:aa:ad:a7:5c:fb:98:a2:71:15:
                    68:e7:8d:0f:71:9a:a1:ca:10:81:f8:f6:85:86:c1:
                    06:cc:a2:47:16:89:ee:d1:90:c9:51:e1:0d:a3:2f:
                    9f:0b
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:10.58.56.18
    Signature Algorithm: sha256WithRSAEncryption
         01:41:2c:91:0b:a1:10:8a:11:1a:95:36:99:2c:27:31:d3:7d:
         e9:4b:29:56:c3:b7:00:8c:f4:39:d2:8c:50:a4:da:d4:96:93:
         eb:bb:71:e3:70:d3:fe:1f:97:b2:bc:5c:f8:f4:65:ed:83:f7:
         67:56:db:0f:67:c2:3d:0c:e7:f8:37:65:1d:11:09:9a:e3:42:
         bc:c6:a0:31:7c:1f:d7:5e:c6:86:72:43:a8:c1:0c:70:33:60:
         dc:14:5b:9d:f3:ab:3d:d5:d2:94:90:1c:ba:fd:80:4d:22:e3:
```

```
31:93:c7:16:5f:85:20:38:ad:36:b9:1a:e0:89:8e:06:8c:f8:
cd:55:cc:a1:89:d3:91:7f:66:61:a3:40:71:c2:1e:ee:3b:80:
37:af:73:5e:8e:0d:db:4b:49:da:a6:bd:7d:0a:aa:9e:9a:9e:
fa:ed:05:25:08:f2:4d:cd:2f:63:55:cf:be:b1:5d:03:c2:b3:
32:bf:f4:7b:1a:10:b9:5e:69:ac:77:5e:4a:4f:85:e3:7f:fe:
04:df:ce:3e:bb:28:8f:e3:bf:1a:f9:0f:94:18:08:86:7d:59:
57:71:0a:97:0d:86:9c:63:e7:0e:48:7d:f0:0e:1d:67:ff:9b:
1d:1b:05:25:c8:c3:1f:f4:52:0f:e1:bf:86:d7:ec:47:10:bd:
94:cf:ca:e2
```

Configure gNMI Certificate

Crosswork Data Gateway acts as the gNMI client while the device acts as gNMI server. Crosswork Data Gateway validates the device using a trust chain. It is expected that you have a global trust chain for all the devices. If you have multiple trust chains, add all the device trust chains (single or multiple vendors) in a single .pem file and upload this .pem file to the Crosswork Certificate Management UI.

✎

Note   You can upload only one gNMI certificate to Crosswork.

To add the gNMI certificate.

Step 1   From the Cisco Crosswork UI, go to **Administration > Certificate Management**.

Step 2   Click the + icon to add the certificate.

Step 3   In **Add Certificate** window, enter the following details:

- **Device Certificate Name** - Enter a name for the certificate.

- **Certificate Role** - Select **Device gNMI Communication** from the drop-down list.

- **Device Trust Chain** - Browse your local file system to the location of the rootCA file and upload it.

Figure 24: Add Certificate Window

Note   If gNMI certificate is already configured and you wish to onboard a device with a different trust chain, update the existing .pem file to include details of the new CA. Select the existing gNMI certificate from the list, click the Edit icon and upload the new .pem file.

Step 4 Click **Save**.

The gNMI certificate gets listed in the configured certificates list when it is added.

Figure 25: Certificates Window

Import and Install Certificates on Devices

This section describes how to import and install certificates on the IOS XR and XE devices. Certificates and trustpoint are only required for secure gNMI servers.

Certificates on a Cisco IOS XR Device

To install certificates on a Cisco IOS XR device.

1. Copy rootCA.pem, device.key, and device.crt to the device under /tmp folder.

2. Log in into the IOS XR device.

3. Use the run command to enter the VM shell.

   ```
   RP/0/RP0/CPU0:xrvr-7.2.1#run
   ```

4. Navigate to the following directory:

   ```
   cd /misc/config/grpc
   ```

5. Create or replace the content of the following files:

   ✎

   Note If TLS was previously enabled on your device, the following files will already be present in which case replace the content of these files as explained below. If this is the first time, you are enabling TLS on the device, copy the files from the /tmp folder to this folder.

   • ems.pem with device.crt

   • ems.key with device.key

   • ca.cert with rootCA.pem

6. Restart TLS on the device for changes to take an effect. This step involves disabling TLS with "no-tls" command and re-enabling it with "no no-tls" configuration command on the device.

Certificates on a Cisco IOS XE Device

The following example shows how to install a certificate on a Cisco IOS XE device:

```
# Send:
Device# configure terminal
Device(config)# crypto pki import trustpoint1 pem terminal password password1

# Receive:
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of rootCA.pem, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% Enter PEM-formatted encrypted private General Purpose key.
% End with "quit" on a line by itself.

# Send:
# Contents of device.des3.key, followed by newline + 'quit' + newline:
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,D954FF9E43F1BA20
<snip>
-----END RSA PRIVATE KEY-----
quit

# Receive:
% Enter PEM-formatted General Purpose certificate.
% End with a blank line or "quit" on a line by itself.

# Send:
# Contents of device.crt, followed by newline + 'quit' + newline:
-----BEGIN CERTIFICATE-----
<snip>
-----END CERTIFICATE-----
quit

# Receive:
% PEM files import succeeded.
Device(config)#

# Send:
Device(config)# crypto pki trustpoint trustpoint1
Device(ca-trustpoint)# revocation-check none
Device(ca-trustpoint)# end
Device#
```

Update Protocol on Device from Cisco Crosswork

After you have configured the gNMI certificate in the Cisco Crosswork, update the device with secure protocol details either from the Cisco Crosswork UI (**Device Management** > **Network Devices**) or by specifying the protocol details as **GNMI_SECURE Port** in the .csv file.

The following image shows the updated secure protocol details for a device.

Figure 26: Edit Device Details Window

Enable gNMI on Device

This section explains how to enable gNMI on the device.

Cisco IOS XR devices

1. Enable gRPC over an HTTP/2 connection.

```
Router#configure
Router(config)#grpc
Router(config-grpc)#port <port-number>
```

The port number ranges from 57344 to 57999. If a port number is unavailable, an error is displayed.

2. Set the session parameters.

```
Router(config)#grpc{ address-family | dscp | max-request-per-user | max-request-total |
 max-streams |
max-streams-per-user | no-tls | service-layer | tls-cipher | tls-mutual | tls-trustpoint
 | vrf }
```

where:

- `address-family:` set the address family identifier type

- `dscp:` set QoS marking DSCP on transmitted gRPC

- `max-request-per-user:` set the maximum concurrent requests per user

- `max-request-total:` set the maximum concurrent requests in total

- `max-streams:` set the maximum number of concurrent gRPC requests. The maximum subscription limit is 128 requests. The default is 32 requests

- `max-streams-per-user`: set the maximum concurrent gRPC requests for each user. The maximum subscription limit is 128 requests. The default is 32 requests

- `no-tls`: disable transport layer security (TLS). The TLS is enabled by default.

- `service-layer`: enable the grpc service layer configuration

- `tls-cipher`: enable the gRPC TLS cipher suites

- `tls-mutual`: set the mutual authentication

- `tls-trustpoint`: configure trustpoint

- `server-vrf`: enable server vrf

3. Enable TPA (Traffic Protection for Third-Party Applications)

```
tpa
vrf default
  address-family ipv4
   default-route mgmt
   update-source dataports MgmtEth0/RP0/CPU0/0
```

Cisco IOS XE Devices

The following example shows how to enable the gNMI server in non-secure mode:

```
Device# configure terminal
Device(config)# gnmi-yang
Device(config)# gnmi-yang server
Device(config)# gnmi-yang port <port value> <The default port is 50052.>
Device(config)# end
Device
```

The following example shows how to enable the gNMI server in secure mode:

Certificates and trustpoint are only required for secure gNMI servers.

```
Device# configure terminal
Device(config)# gnmi-yang server
Device(config)# gnmi-yang secure-server
Device(config)# gnmi-yang secure-trustpoint trustpoint1
Device(config)# gnmi-yang secure-client-auth
Device(config)# gnmi-yang secure-port <port value> <The default port is 50051.>
Device(config)# end
Device
```

Configuring gNMI Bundling for IOS XR

In IOS XR, gNMI bundling is implemented to stitch together several Update messages that are included in the Notification message of a SubscribeResponse message. These messages are sent to the IOS XR device. To bundle the Update messages, you must enable bundling and specify the size of the message in the IOS XR device.

Before you begin

Make sure that you are aware of the following:

- IOS XR release versions 7.81 and later support the gNMI bundling capability. For more information about how the bundling feature works, see Programmability Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.8.x.

- The gNMI bundling capability can only be configured from the device. This option is not available in the Crosswork Interface.

Step 1   Enable the bundling feature using the following command:

```
telemetry model-driven
 gnmi
  bundling
```

The gNMI bundling capability is disabled by default.

Step 2   Specify the gNMI bundling size using the following command:

```
telemetry model-driven
 gnmi
  bundling
   size <1024-65536>
```

The default bundling size is 32768 bytes.

Important   After processing the (N - 1) instance, if the message size is less than the bundling size, it may allow for one more instance, which results in exceeding the bundling size.

What to do next

Verify that the bundling capability is configured using the following:

```
RP/0/RP0/CPU0:R0(config)#telemetry model-driven
RP/0/RP0/CPU0:R0(config-model-driven)#gnmi ?
  bundling   gNMI bundling of telemetry updates
  heartbeat  gNMI heartbeat
  <cr>
RP/0/RP0/CPU0:R0(config-model-driven)#gnmi bundling ?
  size  gNMI bundling size (default: 32768)
  <cr>
RP/0/RP0/CPU0:R0(config-model-driven)#gnmi bundling
RP/0/RP0/CPU0:R0(config-gnmi-bdl)#size ?
  <1024-65536>  gNMI bundling size (bytes)
```

Create a Collection Job from Cisco Crosswork UI

Follow the steps to create a collection job:

Note   Collection jobs created through the Cisco Crosswork UI page can only be published once.

Before you begin
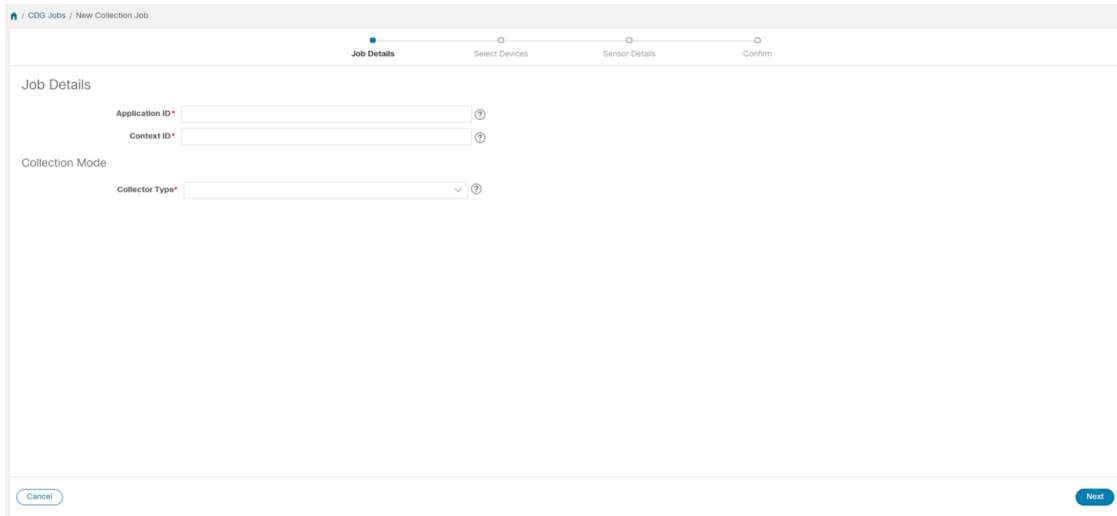
Ensure that a data destination is created (and active) to deposit the collected data. Also, have details of the sensor path and MIB that you plan to collect data from.

Step 1   From the main menu, go to **Administration** > **Collection Jobs** > **Bulk Jobs**

Step 2   In the left pane, click ⊞ button.

Step 3   In the **Job details** page, enter values for the following fields:

Figure 27: Job Details Window
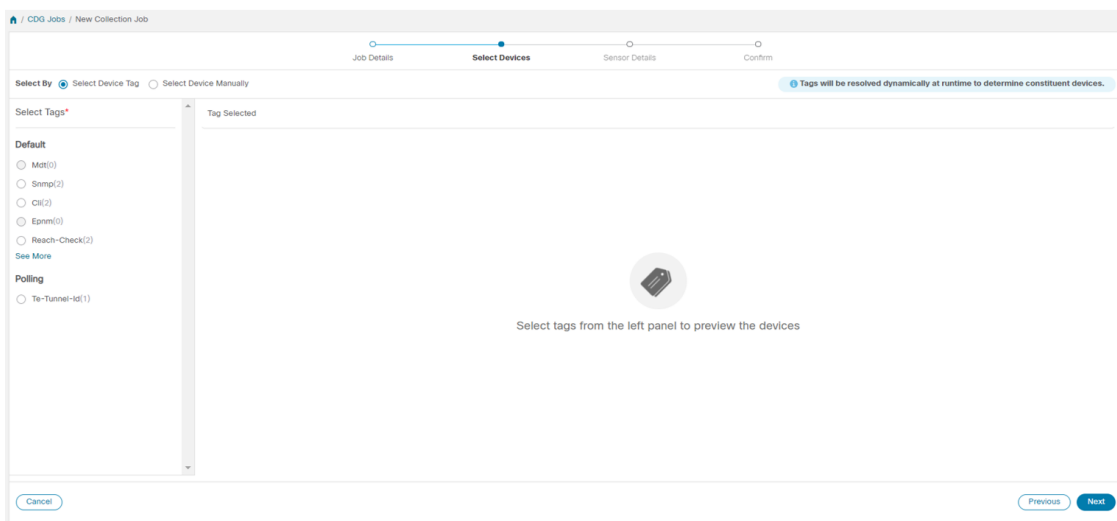
- Application ID: A unique identifier for the application.

- Context: A unique identifier to identify your application subscription across all collection jobs.

- Collector Type: Select the type of collection - CLI or SNMP.

Click **Next**.

Step 4   Select the devices from which the data is to be collected. You can either select based on device tag or manually. Click **Next**.

Figure 28: Select Devices Window

Step 5   (Applicable only for CLI collection) Enter the following sensor details:

Figure 29: Sensor Details Window

- Select data destination from **Select Data Destination** drop-down.

- Select sensor type from **Sensor Types** pane on the left.

If you selected **CLI PATH**, Click ⊞ button and enter the following paramters in the **Add CLI Path** dialog box:

Figure 30: Add CLI Path Dialog Box
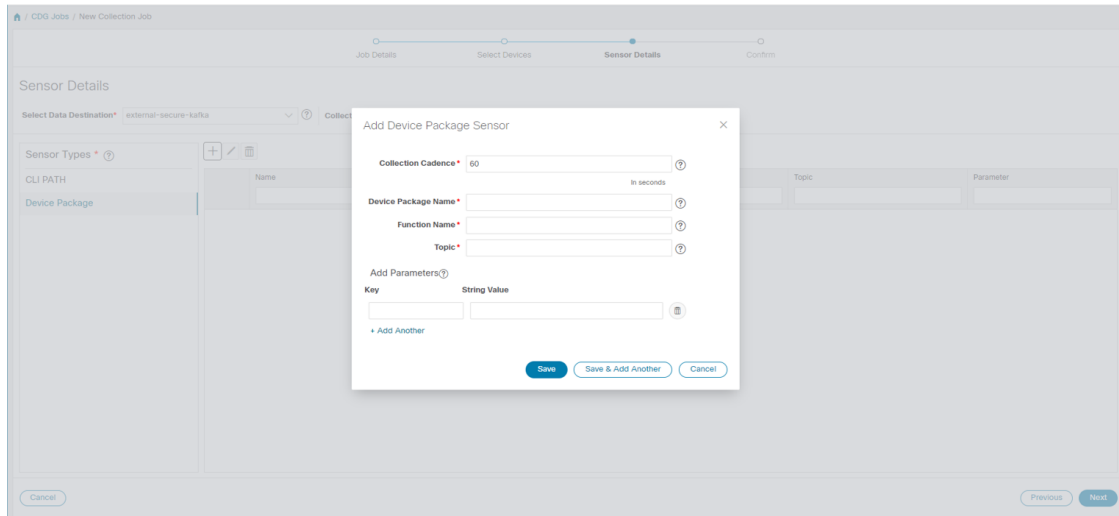
- Collection Cadence: Push or poll cadence in seconds.

- Command: CLI command

- Topic: Topic associated with the output destination.

  Note   Topic can be any string if using an external gRPC server.

If you selected **Device Package**, click ⊞ button and enter values for the following parameters in the **Add Device Package Sensor** dialog box:

Figure 31: Add Device Package Sensor Dialog Box
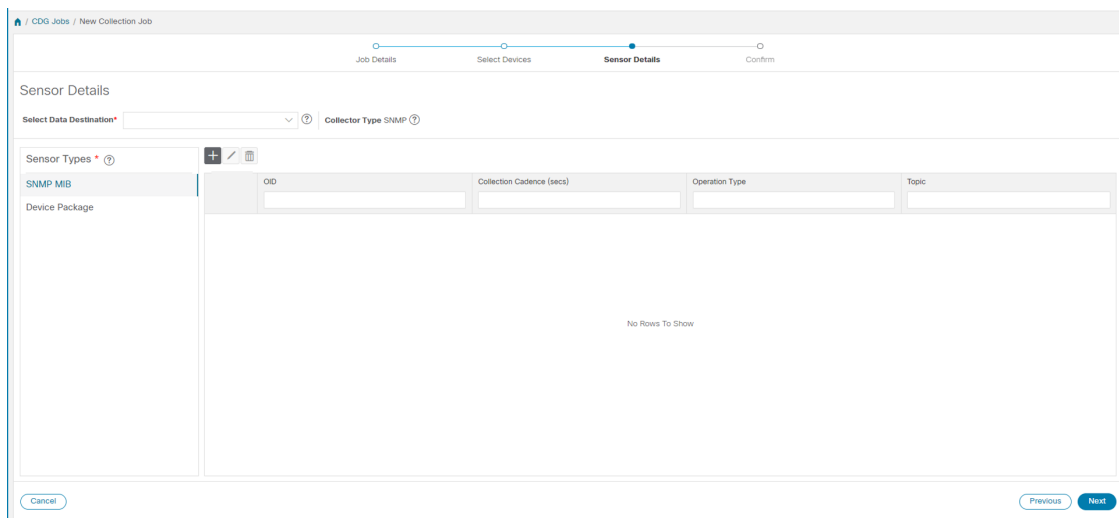
- Collection cadence: Push or poll cadence in seconds.

- Device Package Name: Custom XDE device package ID used while creating device package.

- Function name: Function name within custom XDE device package.

- Topic: Topic associated with the output destination.

Enter Key and String value for the paramters.

Click **Save**.

Step 6   (Applicable only for SNMP collection) Enter the following sensor details:

Figure 32: Sensor Details Window

• Select data destination from **Select Data Destination** drop-down.

• Select sensor type from **Sensor Types** pane on the left.

If you selected **SNMP MIB**, Click ⊞ button and enter the following parameters in the **Add SNMP MIB** dialog box:

Figure 33: Add SNMP MIB Dialog Box
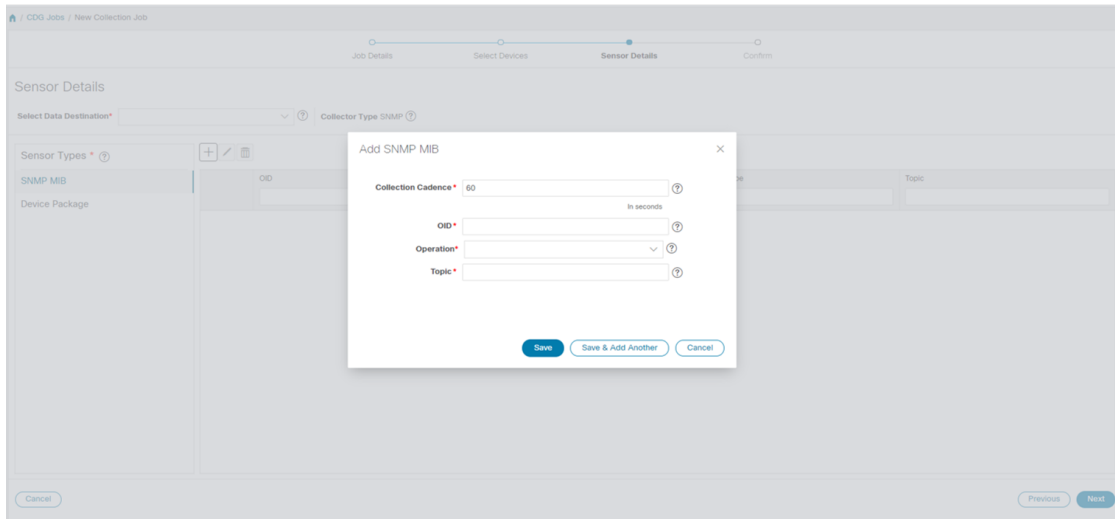
• Collection Cadence: Push or poll cadence in seconds.

• OID

• Operation: Select the operation from the list.

• Topic: Topic associated with the output destination.

If you selected **Device Package**, click ⊞ button and enter values for the following parameters in the **Add Device Package Sensor** dialog box:

Figure 34: Add Device Package Sensor Dialog Box

- Collection Cadence: Push or poll cadence in seconds.

- Device Package Name: Custom device package ID used while creating device package.

- Function name: Function name within custom device package.

- Topic: Topic associated with the output destination.

Enter Key and String value for the parameters.

Click **Save**.

Step 7   Click **Create Collection Job**.

Note   When a collection job is submitted for an external Kafka destination i.e., unsecure Kafka, the dispatch job to Kafka fails to connect. The error seen in collector logs is `org.apache.kafka.common.errors.TimeoutException: Topic cli-job-kafka-unsecure not present in metadata after 60000 ms`. In Kafka logs, the error seen is `SSL authentication error "[2021-01-08 22:17:03,049] INFO [SocketServer brokerId=0] Failed authentication with /80.80.80.108 (SSL handshake failed) (org.apache.kafka.common.network.Selector)`.

This happens because port is blocked on external Kafka VM. You can use the following command to check if port is listening on Kafka docker/server port:

`netstat -tulpn`

Fix the problem on the Kafka server and restart the Kafka server process.

Monitor Collection Jobs

You can monitor the status of the collection jobs currently active on all the Crosswork Data Gateway instances enrolled with Cisco Crosswork from the **Collection Jobs** page.

In the Cisco Crosswork UI, from the left navigation bar, choose **Administration** > **Collection Jobs**.

This left pane lists all active collection jobs along with their Status, App ID, and Context ID. The **Job Details** pane shows the details of all collection tasks associated with a particular job in the left pane. The overall status of the Collection job in the **Collection Jobs** pane is the aggregate status of all the collection tasks in the **Jobs Details** pane.

When you select a job in the **Collection Jobs** pane, the following details are displayed in the **Job Details** pane:

- Application name and context associated with the collection job.

- Status of the collection job.

Note

- The status of a collection task associated with a device after it is attached to a Crosswork Data Gateway, is **Unknown**.

- A job could have status as **Unknown** for one of the following reasons:

  - Crosswork Data Gateway has not yet reported its status.

  - Loss of connection between Crosswork Data Gateway and Cisco Crosswork.

  - Crosswork Data Gateway has received the collection job, but actual collection is still pending. For example, traps are not being sent to Crosswork Data Gateway southbound interface, or device is not sending telemetry updates.

  - The trap condition in a SNMP trap collection job which we are monitoring has not occurred. For example, if you are looking for Link Up or Link down transitions and the link state has not changed since the collector was established, then the state will report as **Unknown**. To validate that trap-based collections are working it is therefore necessary to actually trigger the trap.

- After the collection job is processed, the status changes to 'Successful' if the processing was successful or else it changes to 'Failed'.

- If a collection job is in degraded state, one of the reasons might be that the static routes to the device have been erased from Crosswork Data Gateway.

- Collections to a destination that is in an Error state do not stop. The destination state is identified in background. If the destination is in an Error state, the error count is incremented. Drill down on the error message that is displayed in the **Distribution** status to identify and resolve the issue by looking at respective collector logs.

- Cisco Crosswork Health Insights - KPI jobs must be enabled only on devices mapped to an extended Crosswork Data Gateway instance. Enabling KPI jobs on devices that are mapped to a standard Crosswork Data Gateway instance reports the collection job status as **Degraded** and the collection task status as **Failed** in the **Jobs Details** pane.

- Job configuration of the collection job that you pass in the REST API request. Click ⓘ icon next to **Config Details** to view the job configuration. Cisco Crosswork lets you view configuration in two modes:

  - View Mode

  - Text Mode

- Collection type

- Time and date of last modification of the collection job.

- Collections (x): x refers to requested input collections that span device by sensor paths. The corresponding **(y) Issues** is the count of input collections that are in UNKNOWN or FAILED state.

- Distributions (x): x refers to requested output collections that span device by sensor paths. The corresponding **(y) Issues** is the count of output collections that are in UNKNOWN or FAILED state.

Cisco Crosswork also displays the following details for collections and distributions:

Field	Description
Collection/Distribution Status	Status of the collection/distribution. It is reported on a on change basis from Crosswork Data Gateway. Click ⓘ next to the collection/distribution status for details.
Hostname	Device hostname with which the collection job is associated.
Device Id	Unique identifier of the device from which data is being collected.

Field	Description
Sensor Data	Sensor path Click ⓘ to see collection/distribution summary. From the sensor data summary pop up you can copy the sensor data by clicking **Copy to Clipboard**. Click 📊 to see collection/distribution metrics summary. The metrics are reported on cadence-basis i.e., once every 10 minutes by default. It shows the following metrics for a collection: • last_collection_time_msec • total_collection_message_count • last_device_latency_msec • last_collection_cadence_msec It shows the following metrics for a collection: • total_output_message_count • last_destination_latency_msec • last_output_cadence_msec • last_output_time_msec • total_output_bytes_count
Destination	Data destination for the job.
Last Status Change Reported Time	Time and date on which last status change was reported for that device sensor pair from Crosswork Data Gateway

Note

- `Create Failed` error means out of N devices, some devices failed to setup. However, the collection would happen on the devices that were successfully setup. You can identify the device(s) causing this error by using `Control Status` API.

- If job creation failed on a particular device because of NSO errors, after fixing NSO errors, you have to manually change the administration state of the device first to "Down" and then "Up". However, doing so resets the collection on the device.

Note

Create/Delete failed errors are shown in a different screen pop up. Click ⓘ next to the job status to see details of the error.

• You may also try recreating the job using PUT collection job API with the same payload.

Collection Status for Event-based collection jobs

1. When data collection is successful, status of the Collection job changes from **Unknown** to **Success** in the **Collection Jobs** pane.

2. When a device is detached from the Crosswork Data Gateway, all corresponding collection jobs are deleted and collection job status is displayed as **Success** in the **Collection Jobs** pane. There are no devices or collection tasks displayed in the **Job Details** pane.

3. When a device is attached to a Crosswork Data Gateway, Crosswork Data Gateway receives a new collection job with the status set to **Unknown** that changes to **Success** after receiving events from the device.

4. If the device configuration is updated incorrectly on a device that is already attached to a Crosswork Data Gateway and after the Crosswork Data Gateway has received the job and events, there is no change in status of the collection task in the **Jobs Details** pane.

5. If the device inventory is updated with incorrect device IP, the collection task status in the **Jobs Details** pane is **Unknown**.

Delete a Collection Job

System jobs (default jobs created by various Crosswork Applications) should not be deleted as it will cause issues. Jobs created by Health Insights should only be deleted by disabling the KPI profile which will remove the collection jobs it deployed. Use this procedure to delete external collection jobs from the **Collection Jobs** page.

Follow the steps to delete a collection job:

Step 1 Go to **Administration** > **Collection Jobs.**

Step 2 Select either the **Bulk Jobs** tab or **Parmaterized Jobs** tab.

Step 3 In the **Collection Jobs** pane on the left hand side, select the collection job that you want to delete.

Step 4 Click 🗑.

Step 5 Click **Delete** when prompted for confirmation.

Troubleshoot Crosswork Data Gateway

You can troubleshoot the Crosswork Data Gateway from the UI or from the Interactive Console of the Crosswork Data Gateway VM.

This section explains the various troubleshooting options that are available from the Cisco Crosswork UI.

Figure 35: Data Gateway - Troubleshooting
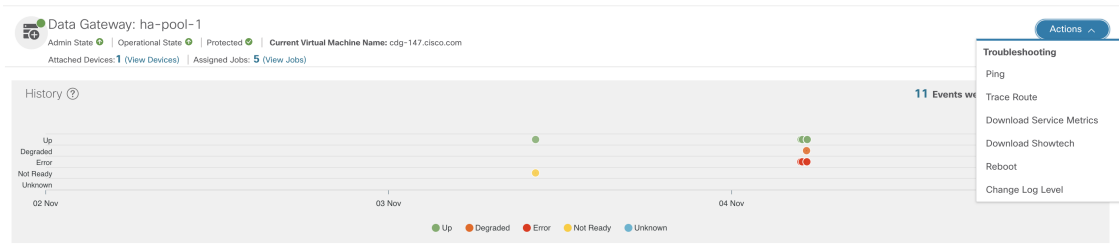
For details on troubleshooting options available from the Interactive Console of the Crosswork Data Gateway VM, see Troubleshooting Crosswork Data Gateway VM.

Check Connectivity to the Destination

To check connectivity to a destination from the Cisco Data Gateway, use the **Ping** and **Traceroute** options from Troubleshooting Menu.

> **Note** Ping traffic should be enabled on the network to ping the destination successfully.

1. Go to **Administration** > **Data Gateway Management** > **Data Gateways**.

2. Click the Cisco Crosswork Data Gateway name from which you want to check the connectivity.

3. In the Crosswork Data Gateway details page, on the top right corner, click **Actions** and choose: **Ping** or **Traceroute**.

   • **Ping** - Enter details in the **Number of Packets**, and **Destination Address** fields and click **Ping**.

   • **Traceroute** - Enter the **Destination Address**, and click **Traceroute**.

4. If the destination is reachable, Cisco Crosswork displays details of the **Ping** or **Traceroute** test in the same window.

Download Service Metrics

Use this procedure to download the metrics for all collection jobs for a Crosswork Data Gateway from the Cisco Crosswork UI.

Step 1 Go to **Administration** > **Data Gateway Management** > **Data Gateways**.

Step 2   Click the Crosswork Data Gateway name for which you want to download the service metrics.

Step 3   In the Crosswork Data Gateway details page, on the top right corner, click **Actions** > **Download Service Metrics**.

Step 4   Enter a passphrase.

>   **Note**   Ensure that you make a note of this passphrase. This passphrase will be used later to decrypt the file.

Step 5   Click **Download Service Metrics**. The file is downloaded to the default download folder on your system in an encrypted format.

Step 6   After the download is complete, run the following command to decrypt it:

>   **Note**   In order to decrpyt the file, you must use openssl version 1.1.1i. Use the command `openssl version` to check the openssl version on your system.

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in <service metrics file> -out <decrypted
filename> -pass pass:<encrypt string>
```

Download Showtech Logs

Follow the steps to download showtech logs from Cisco Crosswork UI:

>   **Note**   Showtech logs cannot be collected from the UI if the Crosswork Data Gateway is in an ERROR state. In the DEGRADED state of the Cisco Crosswork Data Gateway, if the OAM-Manager service is running and not degraded, you will be able to collect logs.

Step 1   Go to **Administration** > **Data Gateway Management** > **Data Gateways**.

Step 2   Click the Crosswork Data Gateway name for which you want to download showtech.

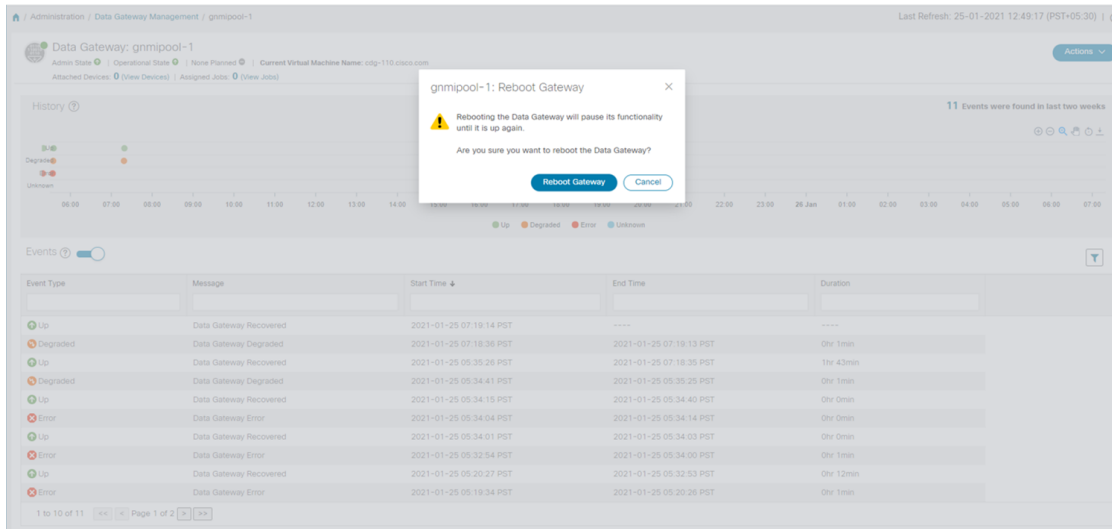Step 3   In the Crosswork Data Gateway details page, on the top right corner, click **Actions** and click **Download Showtech**.

Figure 36: Data Gateway - Download Showtech

Step 4   Enter a passphrase.

Note   Ensure that you make a note of this passphrase. You will need to enter this passphrase later to decrypt the showtech file.

Figure 37: Download Showtech Pop-up Window

Step 5   Click **Download Showtech**. The showtech file downloads in an encrypted format.

Note   Depending on how long the system was in use, it may take several minutes to download the showtech file.

Step 6   After the download is complete run the following command to decrypt it:

Note   In order to decrypt the file, you must use OpenSSL version 1.1.1i. Use the command `openssl version` to check the OpenSSL version on your system.

To decrypt the file on a MAC, you must install OpenSSL 1.1.1+. This is because LibreSSL's `openssl` command does not support all the switches supported by OpenSSL's `openssl` command.

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<encrypt string>
```

Reboot Cisco Crosswork Data Gateway VM

Follow the steps to reboot a Crosswork Data Gateway from Cisco Crosswork UI:

Note   Rebooting the Crosswork Data Gateway pauses its functionality until it is up again.

Step 1   Go to **Administration** > **Data Gateway Management** > **Data Gateways**.

Step 2   Click the Cisco Crosswork Data Gateway name that you want to reboot.

Step 3   In the Crosswork Data Gateway details page, on the top right corner, click **Actions**, and click **Reboot**.

Figure 38: Data Gateway - Reboot

Step 4   Click **Reboot Gateway**.

Figure 39: Reboot Gateway Popup Window

Once the reboot is complete, check the operational status of the Cisco Crosswork Data Gateway in the **Administration** > **Data Gateway Management** > **Data Gateway Instances** window.

Change Log Level of Crosswork Data Gateway Components

Cisco Crosswork UI offers the option to change the log level of a Crosswork Data Gateway's components, for example collectors (cli-collector) and infra services (oam-manager). Log level changes apply only to the Crosswork Data Gateway on which you are making the change.

> **Note** Changing the log level for offload services is not supported.

Step 1 Go to **Administration** > **Data Gateway Management** > **Data Gateways**.

Step 2 Click the Crosswork Data Gateway name on which you wish to change the log level for the collectors of Crosswork Infrastructure services.

Step 3 In the Crosswork Data Gateway details page, on the top right corner, click **Actions** > **Change Log Level**.

The **Change Log Level** window appears, indicating the current log level of each container service.

Figure 40: Change Log Level Window

Change Log Level: ha-pool-1   ✕

Selected 0 / Filtered 0 / Total 66

| Change Log Level ∨ | Reset to Default | | ▼ |

	Container Service Name ↑	Component	Log Level
☐	cli collector	grpc	Info
☐	cli collector	xde runtime	Error
☐	cli collector	xde cli_transport	Error
☐	cli collector	dispatcher	Info
☐	cli collector	kafka	Info
☐	cli collector	xde function	Error
☐	cli collector	all	Info
☐	cli collector	xde session	Error
☐	cli collector	xde snmp	Error
☐	cli collector	spring web	Info
☐	cli collector	netty	Info
☐	cli collector	coordinator	Info
☐	controller gateway	all	Info
☐	gnmi collector	spring web	Info

Save   Discard Changes   Cancel

Step 4   Select the check box of the container service for which you wish to change the log level.

Step 5   From the **Change Log Level** drop-down list at the top of the table, select a log level from **Debug**, **Trace**, **Warning**, **Info** and **Error**.

> **Note**   To reset the log level of all logs to the default log level (**Info**), click **Reset to Default**.

Step 6   Click **Save** to save the log level change.

After you click **Save**, a UI message appears indicating that the log level of the component was changed successfully.

Network Load Balancer Displays Incorrect Health Status for Active Crosswork Data Gateway

During the pool creation, Crosswork Data Gateway opens a health port for Network Load Balancer (NLB) to indicate Crosswork Data Gateway's health status. However, if the NLB FQDN resolves to IP addresses that are on different subnets of eth2 then Crosswork Data Gateway adds a static route to VM. The inclusion of the static route may fail with an error due to network configuration issues. Crosswork Data Gateway disregards the failure and creates the HA pool. As a consequence, Crosswork Data Gateway does not collect any data from the device.

To resolve this issue, use the following procedure:

Step 1 Log in to the system identified as NLB and view the health status of the Crosswork Data Gateway.

Step 2 If status is unhealthy, verify if the NLB subnet address conflicts with the interfaces such as eth1 or eth0. To resolve the conflict, perform one of the following:

- Modify the NLB IP addresses and restart the Infra services (oam-manager).

- Redeploy the Crosswork Data Gateway VMs using new subnet configurations.

Collection Job Status on the Collection Jobs Page is in the DEGRADED State

If a collection job on the Collection Jobs page is in the DEGRADED state, check the **Service Status** table on the **Administration** > **Data Gateway Management** > **Data Gateways** > (click){Crosswork Data Gateway} page. This table provides the list of services on the system and the collector that is responsible for running the job.

If the collector is not listed, use the following procedure:

Step 1 Go to the Main Menu on the interactive console and select the **Troubleshooting** menu.

Step 2 Select the **Remove All Non-Infra Containers and Reboot the VM** menu.

Step 3 In the confirmation box, select **Yes**.

Collection Job Status on the Collection Jobs Page is in the DEGRADED State

If a collection job on the Collection Jobs page is in the DEGRADED state, check the **Service Status** table on the **Administration** > **Data Gateway Management** > **Data Gateways** > (click){Crosswork Data Gateway}

page. This table provides the list of services on the system and the collector that is responsible for running the job.

If the collector is not listed, use the following procedure:

Step 1 Go to the Main Menu on the interactive console and select the **Troubleshooting** menu.

Step 2 Select the **Remove All Non-Infra Containers and Reboot the VM** menu.

Step 3 In the confirmation box, select **Yes**.