Cisco Crosswork Data Gateway

This section contains the following topics:

Overview of 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 Crosswork Network Controller 6.0 release.

The number and deployment profiles (Standard or Extended) of Crosswork Data Gateways, also refered to as data gateways, you need depends on the number of devices supported, the amount of data being processed, the frequency at which it’s collected, and the network architecture.

When data gateway is deployed with 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**: A Crosswork Data Gateway or a data gateway instance that you install.

- **Crosswork Data Gateway Profile**: 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 data gateway in your data center.

- **Crosswork Data Gateway Pool**: A logical unit of one or more data gateway instances with an option to enable high availability. When a data gateway instance goes down, Cisco Crosswork automatically replaces the instance with a spare instance from the pool to ensure that data collections have minimal disruption.
- **Crosswork Data Gateway**: A data gateway instance that is assigned a virtual IP address when it is added to a data gateway pool.

  Operations such as attaching or detaching devices, creating collection jobs happen on the data gateway.
- **Data Destination**: Internal or external recipients of data collected by the 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 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.

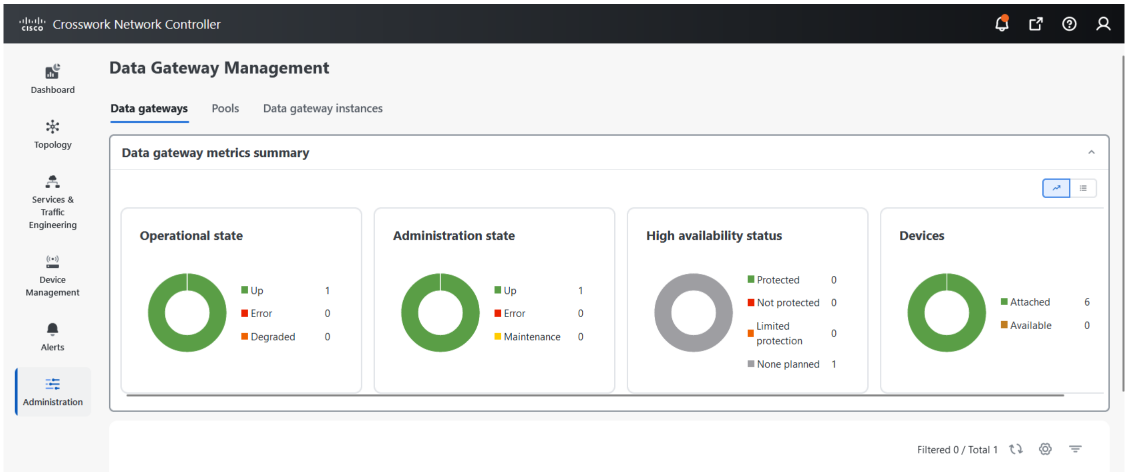
Note This chapter explains only the data gateway features that can be accessed via Cisco Crosswork UI.

For more information about the Interactive Console of the data gateway instance and how to manage it, see **Appendix A**: Configure Crosswork Data Gateway Instance.

Crosswork Data Gateway UI Overview

To open the 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 data gateways in the network. You can attach or detach devices to the Data Gateway from this tab.
- **Pools**: Manages the data gateway pools.
- **Data gateways instances**: Manages virtual the 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 which columns will 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 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: Crosswork Data Gateway UI

Column	Description
Operational State	Operational state of the data gateway instance. A data gateway instance has the following operational states: • **Degraded**: The data gateway instance is reachable but one or more of its components are in a state other than OK. • **Up**: The data gateway instance is operational and all individual components are "OK". • **Error**: The data gateway instance is unreachable or some of its components are in Error state.
Administration state	Administration state of the data gateway instance. The state could be any of the following: • **Up**: The instance is administratively up. • **Maintenance**: Operations between Cisco Crosswork and the data gateway are suspended to perform upgrades or other maintenance activities (for example, uploading certificates).
High availability status	High availability status of a 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 data gateway pool.

Column	Description
Name	Name of the 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 data gateway. • Data Gateway Instance UUID Click the instance name to open the data gateway vitals page. The page displays the operations and health summary of a data gateway.
Pool name	Name of the data gateway pool. On clicking the pool name, the data gateway vitals page opens.
Site name	Site to which the data gateway instance is assigned. **Note** This column is only displayed with the geo redundancy feature is enabled. For information on the geo redundancy capabilities, see the *Enable Geo Redundancy* section in *Cisco Crosswork Network Controller 7.0 Installation Guide*.
Data gateway instance role	Indicates the current role of the data gateway instance. The role could be any of the following: • **Assigned**: The data gateway instance is attached to a pool. • **Unassigned**: The data gateway instance is not attached to any pool. • **Spare (Active)**: The data gateway instance is a spare instance that can be used during a failover process in an active site. • **Spare (Standby)**: The data gateway instance acts as a spare instance for failover procedures in a standby site.

Column	Description
Outage history	Outage history of the 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 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 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 data gateway was not in Error or Degraded state and was only Up, then the tile is Green.
Average availability	Value indicating the health of the data gateway instance. This percentage is calculated as the total time (in milliseconds) a 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 the last event is the current time stamp, so the duration of the last event is between its start time and the current time stamp.

Column	Description
Data gateway instance name	Name of the data gateway that is created automatically when you add a 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: • Instance name • Description • Instance type • Instance role • CPU • Memory • Number of NICs • Instance UUID • Instance OS version • Interface name • Interface role(s) • Interface mac • Interface name The **Additional interface role information** describes the interface roles available in data gateway.
Attached device count	Indicates the number of the devices that are attached to the data gateway pool.
PDG identifier	Unique identifier of the physical 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 19. • Detach devices. For more information, see Manage Crosswork Data Gateway Device Assignments, on page 27. • Move devices. For more information, see Manage Crosswork Data Gateway Device Assignments, on page 27. • Initiate a failover. For more information, see Perform a Manual Failover, on page 18.

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 data gateway instances and pools. For information on using Dashboard, see Overview of the Topology Map.

Set Up Crosswork Data Gateway To Collect Data

Before setting up the data gateways, it's essential to have a good understanding of how Crosswork must be setup. For more information, see Setup Workflow.

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

Note This workflow assumes that you have already installed Crosswork Data Gateway as explained in *Cisco Crosswork Network Controller 7.0 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.

The following tasks are listed according to the default configuration that Crosswork supports for Cisco devices. Optional tasks are only required if you wish to use the advanced features.

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

Task	Follow the steps in...
1. Create data gateway pools.	Create a Data Gateway Pool, on page 10
2. (Optional) Create data gateway pools in the geo redundancy-enabled sites.	Create a Pool in the Geo Redundancy-Enabled Sites, on page 14
2. Attach devices to the data gateway.	Attach Devices to a Crosswork Data Gateway, on page 19
3. Verify that the default collection jobs are created and running successfully.	Monitor Collection Jobs, on page 86
4. (Optional) Extend device coverage to collect data from currently unsupported devices or third-party devices.	Device Packages, on page 40
5. (Optional) Forward data to the external data destinations.	Create and Manage External Data Destinations, on page 33
6. (Optional) Create custom collection jobs that are independent of the ones that are built by Cisco Crosswork.	Crosswork Data Gateway Collection Jobs, on page 49

Crosswork Data Gateway High Availability with Pools

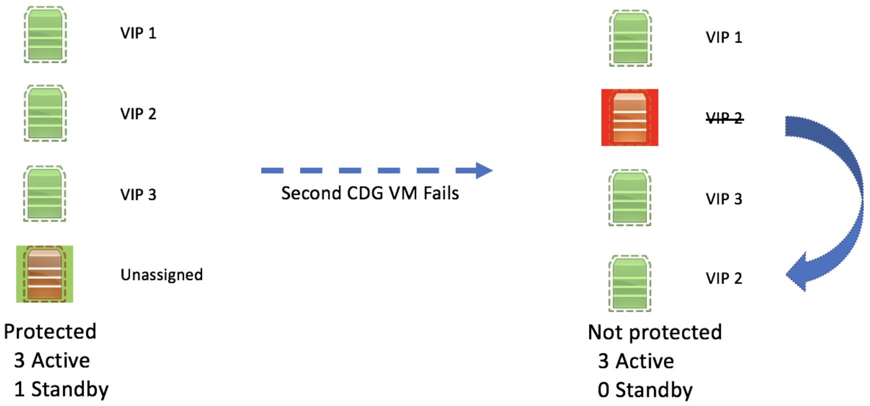
A Crosswork Data Gateway pool ensures that your device-specific data collection occurs with minimal disruption.

A pool can consist of one or more data gateway instances with an option to enable high availability.

If a data gateway instance in the pool goes down, Cisco Crosswork automatically replaces that instance with a standby instance from the pool (failover) or lets you manually initiate a failover. For information on how to initiate a failover, see Perform a Manual Failover, on page 18.

A 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. When 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 data gateway instance in a pool has the same Southbound IP address, reboot the standby data gateway, so that the standby data gateway instance loses its southbound IP address when it comes up.

For example, CDG1 (active) with southbound IP address becomes unresponsive due to port failures or cable disconnections. Crosswork Network Controller detects this and activates CDG2 (standby) to replace CDG1. At that point, CDG1 and its replacement have the same device facing IP address. Thus, it is essential to power off any failed data gateway (via VMware) to avoid conflicts until the issue causing the unresponsiveness is addressed and it can rejoin the pool.

A Crosswork Data Gateway pool has the 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 an 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 data gateway manager conducts regular heartbeat or liveliness checks of each enrolled data gateway at 10-second intervals. If the data gateway does not respond within the 6 liveliness checks (taking about 60 seconds), the data gateway manager assumes that the data gateway is in the **ERROR** state.

If the data gateway notes interface connectivity issues for northbound communication within its own health status, it may also respond to the liveliness check and report an **ERROR** state.

The data gateway manager checks the Operational State of the data gateway every 20 seconds. When the active instance is in the **ERROR** state, the data gateway manager initiates a failover, resulting in a spare instance from the pool becoming the new active instance.

Create a Data Gateway Pool

Before you begin

Before creating a data gateway pool, ensure that you are aware of the following:

- Certain fields and configuration options are only accessible with the geo redundancy feature enabled. For information about the geo redundancy capabilities, see the *Enable Geo Redundancy* section in *Cisco Crosswork Network Controller 7.0 Installation Guide*.
- **Enable FQDN for secure syslog communication** data gateway supports secure syslog communication to devices which require the syslog certificate to contain the hostname or FQDN instead of the virtual IP address of the data gateway. This is an optional feature that can be enabled for devices which mandate having the hostname or FQDN in the syslog certificate. If enabled, Cisco Crosswork fetches the hostname or FQDN for each virtual IP address of the 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 data gateway. For details on how to configure secure syslog on devices, see Configure Secure Syslog on Device, on page 67.
- Have network information such as virtual IP address (one virtual IP for each active data gateway), subnet mask and gateway information ready.

  Note For 3-NIC deployment, you must also provide the gateway address that is used to access the network devices.

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

  - An additional IP address on the Data Network for 2 NIC deployment.
  - An IP address on the Southbound Network for 3 NIC deployment.
- Decide if you wish to enable 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.
- Make sure you have installed a minimum of one data gateway or, if you prefer high availability, at least two data gateways. The number of data gateways is determined by your network requirements. If you need assistance, contact the Cisco Customer Experience team.

- Ensure that there is at least one data gateway that is registered with Crosswork Network Controller, with the operational state set as **NOT_READY**. For high availability configuration, it is essential to have multiple data gateways.
- An imbalanced pool lacks safeguards against Crosswork or site failure, so ensure that the pool are balanced.

Pool UI terminologies

We recommend that you gain an understanding of these UI controls to make informed selections when creating a pool.

- Crosswork enables you to create custom pool types specific to your data center. For VMware, you can create pools based on VIPs, while for Amazon EC2 and cloud-based deployment, create pools using FQDN.
  - **VIP-based**: The network devices connect to data gateway instances that are part of a HA pool that is located on a single IP subnet. The subnet can be either intra-DC (Data Center) or inter-DC extended.
  - **FQDN-based**: The pool where network devices connect to data gateway instances spans multiple subnets within the same HA pool. To protect the internal subnet addresses of the data gateway HA pool, use an external Network Load Balancer (NLB) that acts as a host for a VIP, directing traffic toward the network devices.
- When selecting the VIP configuration, you have to select one of the following:
  - **Shared VIP**: If the VIPs for the Active and Standby sites are in the same subnet, you can choose the Shared VIP option. This means that the VIPs for the data gateways in both sites are shared and can be found in the Global Pool Parameters pane.
  - **Site Specific VIP**: If the VIPs for the Active and Standby sites are in different subnets, you should select the Site-Specific VIP option. In this situation, the data gateways in each site have separate VIPs and must be configured in their respective site panes.

Pool creation guidelines

When setting up a data gateway pool, it's important to adhere to these guidelines to ensure seamless creation of pools.

- Create at least one pool and assign data gateway instances to it. This step is mandatory to set up the data gateway for collection.
- All the data gateway instances in a pool must be of the same configuration (either Standard, or Extended).
- Pool creation fails if the FQDN configurations are missing for VIPs in the DNS server. Either check the FQDN configuration in the DNS server or disable the FQDN option and try again.
- If you have deployed the VMs on Amazon EC2, all the data gateway instances in a pool must be from the same availability zone.
- If Crosswork is deployed on a dual-stack, make sur that the data gateways are also deployed on a dual-stack to ensure smooth data transmission between them. For dual-stack deployment, create a pool with both VIP IPv4 and IPv6 addresses.

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 one of the following:

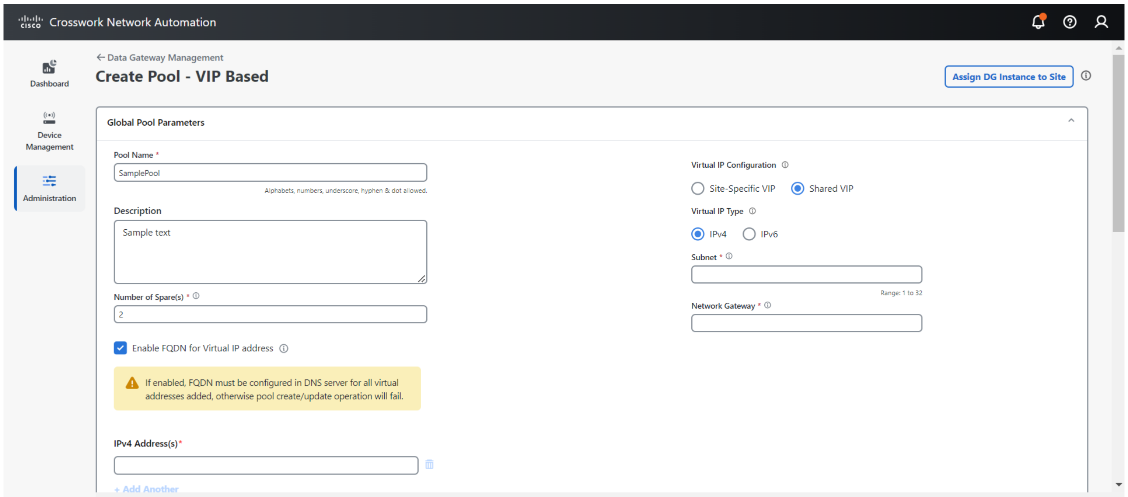
- **VIP-based**
- **FQDN-based**

For information on the pool types, on the top-right, click **Types of pools**. The **Create pool** page opens.

Step 3 In the **Pool parameters** pane, enter the appropriate parameter values based on whether you have chosen a VIP-based or FQDN-based pool.

- **Pool name**: A unique name that suitably describes the network.
- **Description**: A description of the pool.
- **IPv4 subnet**: Subnet mask for each data gateway. IPv4 subnet mask ranges from 1 to 32 and port ranges from 1024 to 65535.
- **IPv4 network gateway**: The data gateway uses the IPv4 network gateway address to communicate with the devices.
- **IPv6 subnet**: Subnet mask for each data gateway. IPv4 subnet mask ranges from 1 to 128 and port ranges from 1024 to 65535.
- **IPv6 network gateway**: The data gateway uses the IPv6 network gateway address to communicate with the devices.
- **Number of spare(s)**: Number of data gateways that operate as the standby instances. When an active data gateway is unavailable, the spare gateway assumes the role of the active gateway.
- (Optional) **Enable FQDN for virtual IP addresses**: Select this option to use hostname or FQDN for each virtual IP address of the data gateway in the syslog certificate.
- **IPv4 address(s)**: Specify the IPv4 address of the data gateway VMs.
- **IPv6 address(s)**: Specify the IPv6 address of the data gateway VMs while ensuring that it is not assigned to any another VM.
- **FQDN**: Specify the FQDN address.

Figure 3: VIP-based Pool Creation Window for Single Stack Deployment


Crosswork Network Automation
Dashboard
Device Management
Administration
← Data Gateway Management
Assign DG Instance to Site
+ Add Another

Create Pool - VIP Based

Global Pool Parameters

Pool Name * SamplePool

Alphabets, numbers, underscore, hyphen & dot allowed.

Description: Sample text

Number of Spare(s) * 2

☑ Enable FQDN for Virtual IP address

If enabled, FQDN must be configured in DNS server for all virtual addresses added, otherwise pool create/update operation will fail.

IPv4 Address(s)*

Virtual IP Configuration: ○ Site-Specific VIP ● Shared VIP

Virtual IP Type: ● IPv4 ○ IPv6

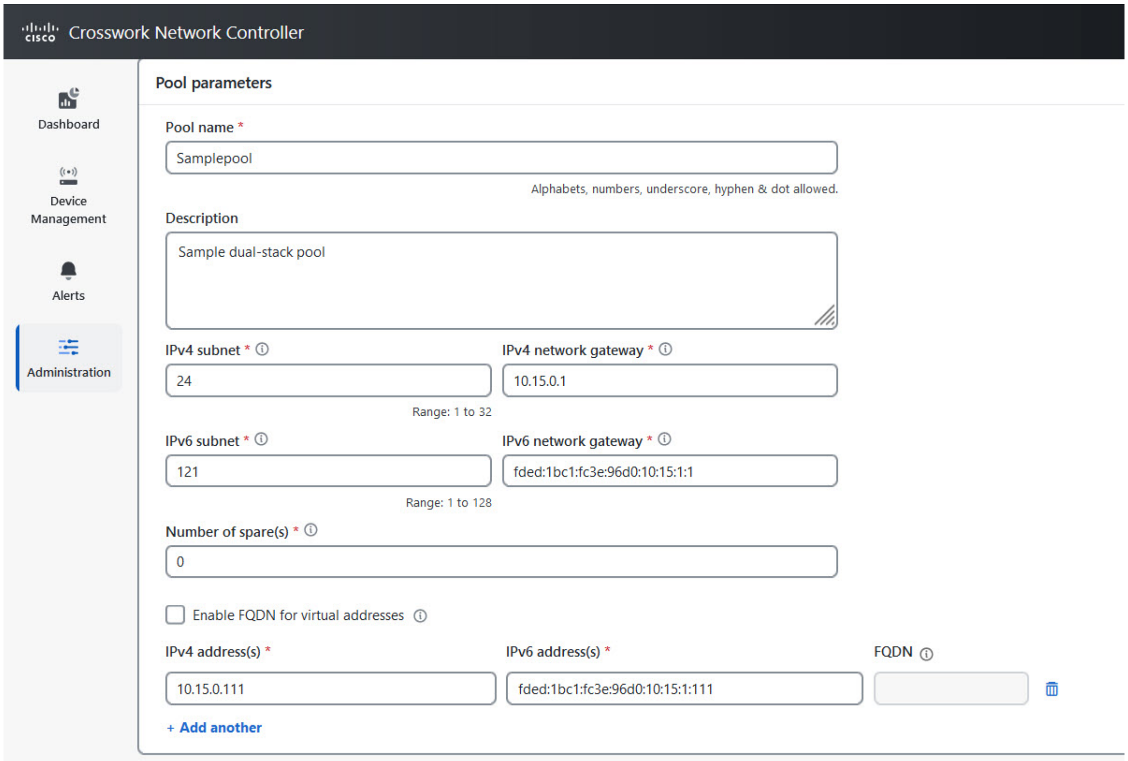
Subnet *

Range: 1 to 32

Network Gateway *

When creating a pool for a dual-stack deployment, you must provide both the VIP IPv4 and IPv6 addresses.

Figure 4: VIP-based Pool Creation Window for Dual-Stack Deployment



Pool parameters

Pool name *: Samplepool

Alphabets, numbers, underscore, hyphen & dot allowed.

Description: Sample dual-stack pool

IPv4 subnet *: 24 (Range: 1 to 32)

IPv4 network gateway *: 10.15.0.1

IPv6 subnet *: 121 (Range: 1 to 128)

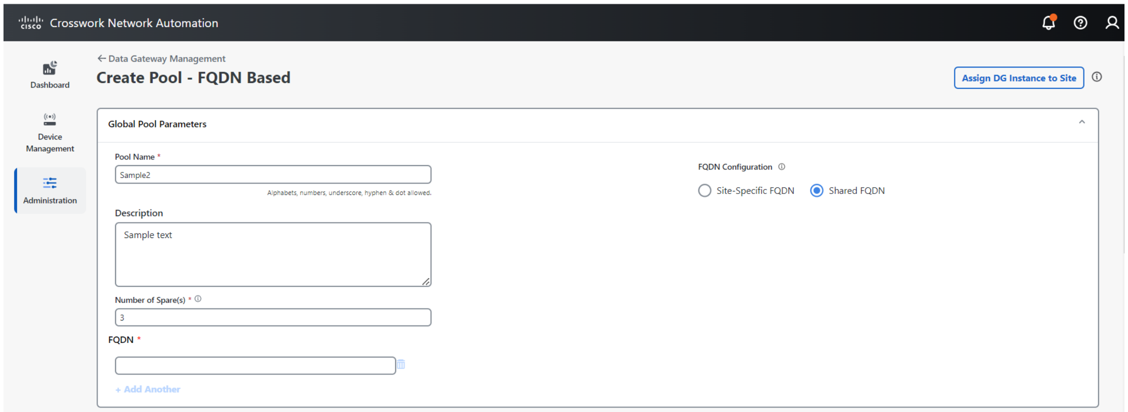
IPv6 network gateway *: fded:1bc1:fc3e:96d0:10:15:1:1

Number of spare(s) *: 0

□ Enable FQDN for virtual addresses

IPv4 address(s) *	IPv6 address(s) *	FQDN
10.15.0.111	fded:1bc1:fc3e:96d0:10:15:1:111	

Figure 5: FQDN-based Pool Creation Window


Crosswork Network Automation
Dashboard
Device Management
Administration
← Data Gateway Management
Assign DG Instance to Site
+ Add Another

Create Pool - FQDN Based

Global Pool Parameters

Pool Name *: Sample2

Alphabets, numbers, underscore, hyphen & dot allowed.

Description: Sample text

Number of Spare(s) *: 3

FQDN *:

FQDN Configuration: ○ Site-Specific FQDN ● Shared FQDN

Step 4 **+ Add another**: Based on the address family you chose earlier (IPv4 or IPv6, or both, FQDN), enter a virtual IP address or FQDN for every active data gateway instance.

If you are creating a pool in the geo redundancy-enabled deployment, from here on follow the procedure in Create a Pool in the Geo Redundancy-Enabled Sites, on page 14. For non-geo deployment, continue with the steps in this document.

Step 5 In the **Assign data gateway instance(s)** pane, select the data gateways from **Unassigned data gateway instance(s)** on the left and click the right arrow to move the instances to **Assigned data gateway instance(s)**.

Step 6 Click **Create**.

In Amazon EC2, after a pool is created, make sure that the NLB is in a healthy state for the active data gateway.

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

Create a Pool in the Geo Redundancy-Enabled Sites

When creating a pool for a geo redundancy enabled deployment, there are some additional VIP and site parameters that must be provided. The pool creation process is similar to a non-geo deployment, but with added fields that only appear when the geo redundancy feature is enabled.

The following procedure describes how to configure the additional fields.

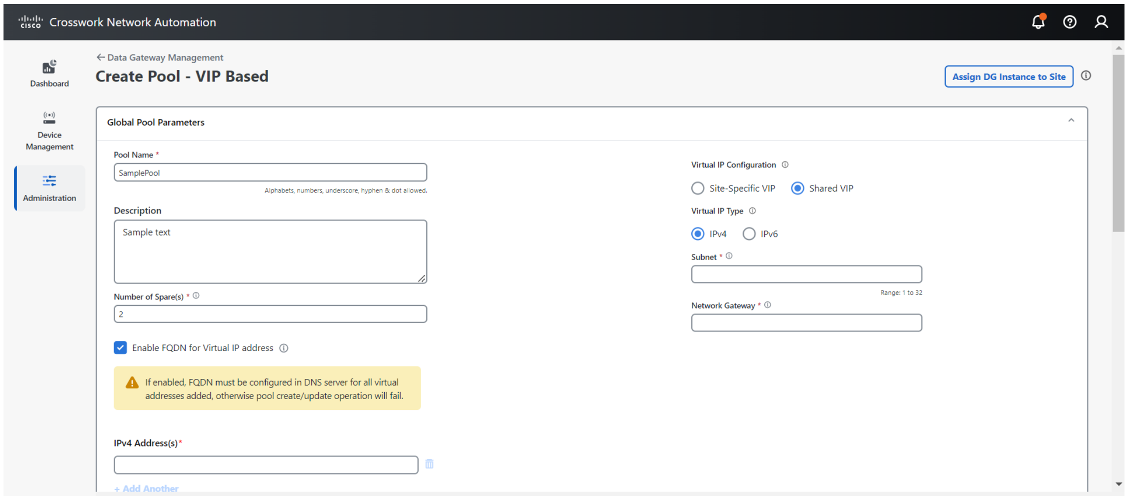
Before you begin

Ensure that you have completed the **steps 1- 4** provided in Create a Data Gateway Pool before proceeding.

Step 1 In the **Pool parameters** page, the following virtual IP options appear based on the type of pool that you want to create:

- **VIP-based pool**:
    - Under **Virtual IP configuration**, select **Shared VIP** or **Site-specific VIP**.
    - If you have selected **Shared VIP**, enter the following:
        - **Virtual IP type**: Select either an IPv4 or IPv6 address family for virtual IPs.
        - For dual stack deployment, specify the IPv4 and IPv6 address family for virtual IPs.
        - **Subnet**: Subnet mask for each data gateway. IPv4 subnet mask ranges from 1 to 32 and port ranges from 1024 to 65535.
        - **Network cateway**: The address using which the data gateway communicates with the devices.
    - If you have selected **Site-specific VIP**, specify **Virtual IP type** by selecting either an IPv4 or IPv6, or dual stack address family for virtual IPs.

Figure 6: VIP-Based Pool Creation Window


Crosswork Network Automation
Dashboard
Device Management
Administration
← Data Gateway Management
Assign DG Instance to Site
+ Add Another

Create Pool - VIP Based

Global Pool Parameters

Pool Name *: SamplePool

Alphabets, numbers, underscore, hyphen & dot allowed.

Description: Sample text

Number of Spare(s) *: 2

☑ Enable FQDN for Virtual IP address

⚠ If enabled, FQDN must be configured in DNS server for all virtual addresses added, otherwise pool create/update operation will fail.

IPv4 Address(s)*

Virtual IP Configuration: ○ Site-Specific VIP ● Shared VIP

Virtual IP Type: ● IPv4 ○ IPv6

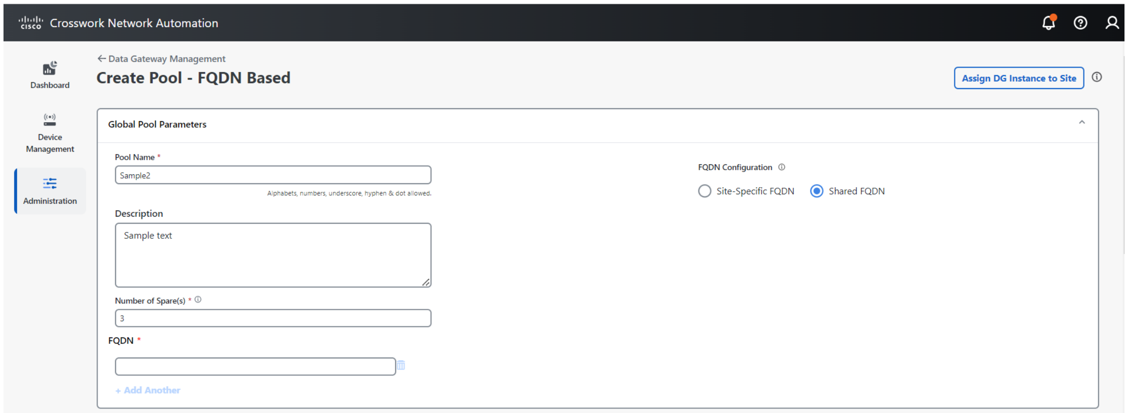
Subnet *

Range: 1 to 32

Network Gateway *

- **FQDN-based pool**:
  - Under **FQDN configuration**, select **Shared FQDN** or **Site-specific FQDN**.
  - If you have selected **Shared FQDN**, enter the following:
    - **Virtual IP type**: Select either an IPv4 or IPv6 address family for virtual IPs.
    - **Subnet**: Subnet mask for each data gateway. IPv4 subnet mask ranges from 1 to 32 and ports range from 1024 to 65535.
    - **Network gateway**: The address using which the data gateway communicates with the devices.
  - If you have selected **Site-specific FQDN**, specify the FQDN.

Figure 7: FQDN-based Pool Creation Window


Crosswork Network Automation
Dashboard
Device Management
Administration
← Data Gateway Management
Assign DG Instance to Site
+ Add Another

Create Pool - FQDN Based

Global Pool Parameters

Pool Name *: Sample2

Alphabets, numbers, underscore, hyphen & dot allowed.

Description: Sample text

Number of Spare(s) *: 3

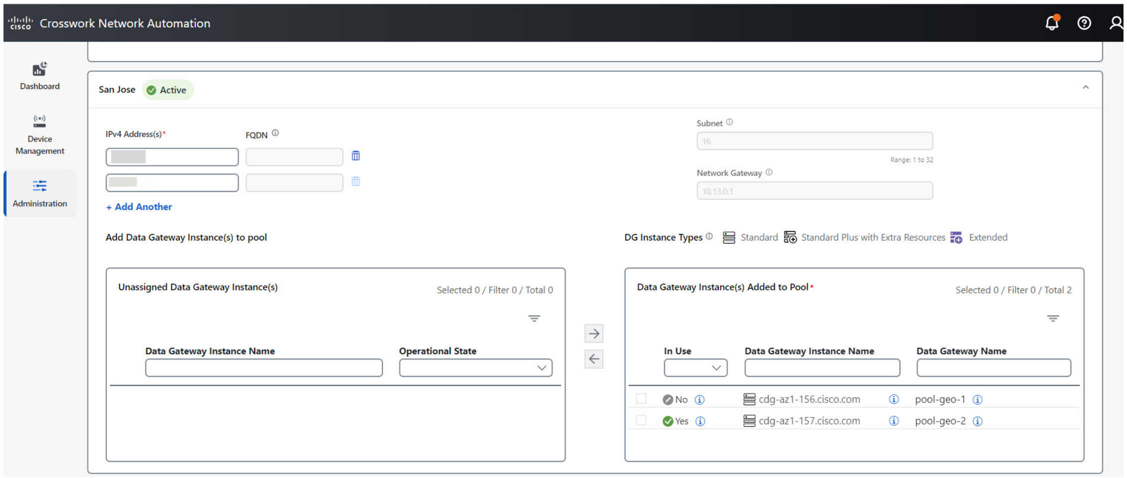
FQDN *

FQDN Configuration: ○ Site-Specific FQDN ● Shared FQDN

Step 2 **+ Add another**: Based on the address family you chose earlier (Dual stack, IPv4 or IPv6, FQDN), enter a virtual IP address or FQDN for every active data gateway instance.

Step 3 In the **Assign data gateway instance(s)** pane, select the data gateways from **Unassigned data gateway instance(s)** on the left and click the right arrow to move the instances to **Assigned data gateway instance(s)**.

Figure 8: Active Pane for Single Stack



Crosswork Network Automation

Dashboard
Device Management
Administration

San Jose ✓ Active

IPv4 Address(s)*   FQDN

+ Add Another

Subnet: 16 (Range: 1 to 32)

Network Gateway: 10.13.0.1

Add Data Gateway Instance(s) to pool

DG Instance Types: Standard | Standard Plus with Extra Resources | Extended

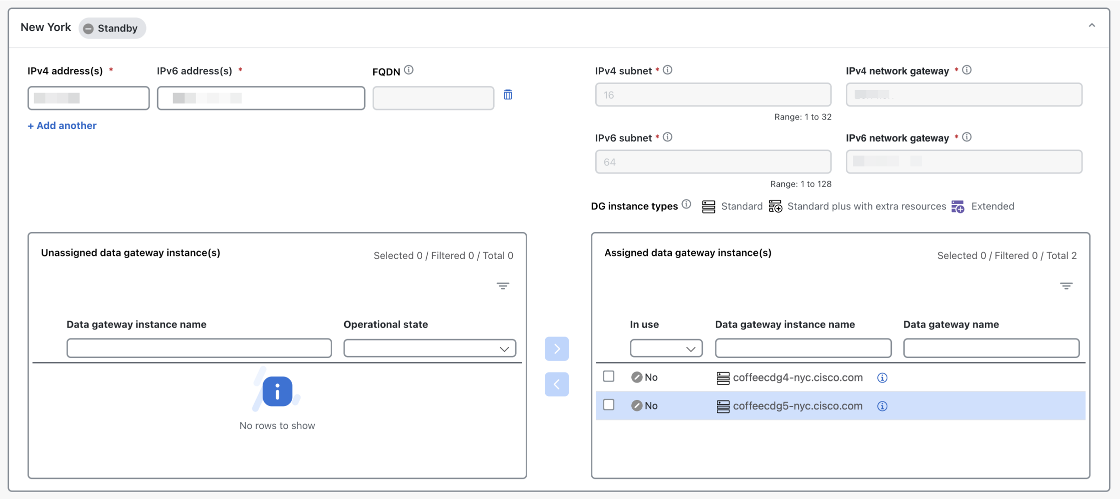
Unassigned Data Gateway Instance(s) — Selected 0 / Filter 0 / Total 0

Data Gateway Instance Name	Operational State

Data Gateway Instance(s) Added to Pool* — Selected 0 / Filter 0 / Total 2

In Use	Data Gateway Instance Name	Data Gateway Name
No	cdg-az1-156.cisco.com	pool-geo-1
Yes	cdg-az1-157.cisco.com	pool-geo-2

Figure 9: Active Pane for Dual Stack



New York — Standby

IPv4 address(s) *   IPv6 address(s) *   FQDN

+ Add another

IPv4 subnet *: 16 (Range: 1 to 32)

IPv4 network gateway *

IPv6 subnet *: 64 (Range: 1 to 128)

IPv6 network gateway *

DG instance types: Standard | Standard plus with extra resources | Extended

Unassigned data gateway instance(s) — Selected 0 / Filtered 0 / Total 0

Data gateway instance name	Operational state

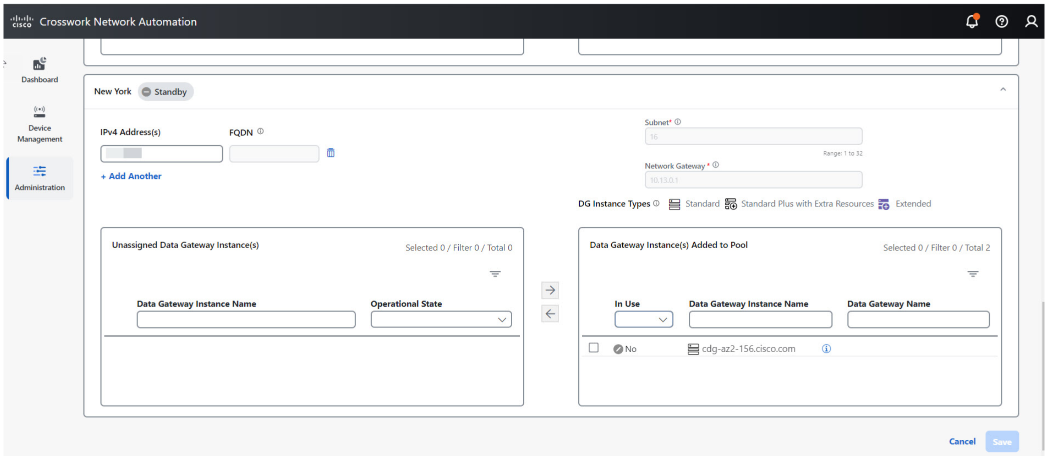
No rows to show

Assigned data gateway instance(s) — Selected 0 / Filtered 0 / Total 2

	In use	Data gateway instance name	Data gateway name
□	No	coffeecdg4-nyc.cisco.com	
□	No	coffeecdg5-nyc.cisco.com	

Step 4 In the **Standby** pane, select the data gateway instances from **Unassigned data gateway Instance(s)** on the left and click the right arrow to move the instances to **Data gateway instance(s) added to pool**.

Figure 10: Standby Pane for Single Stack



New York Standby

IPv4 Address(s)

FQDN

Subnet* 16

Range: 1 to 32

Network Gateway * 10.13.0.1

DG Instance Types Standard Standard Plus with Extra Resources Extended

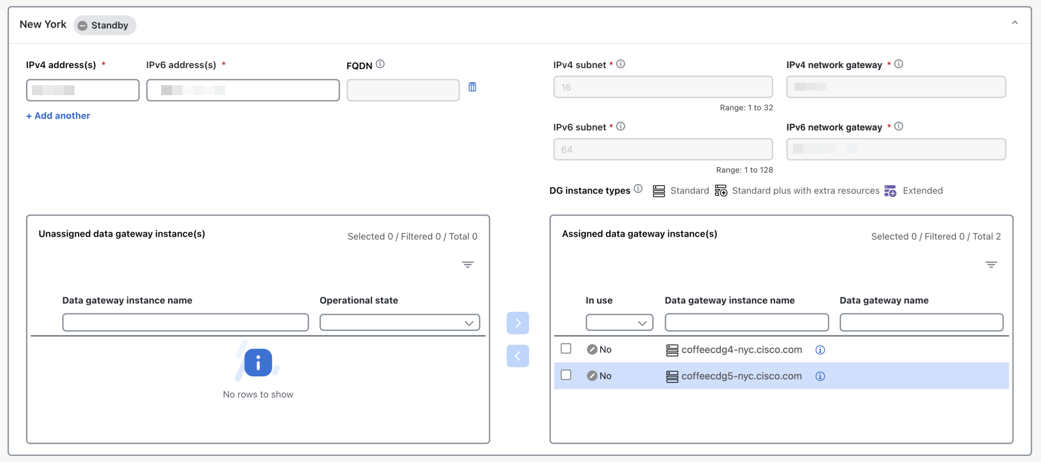
Unassigned Data Gateway Instance(s) Selected 0 / Filter 0 / Total 0

Data Gateway Instance Name	Operational State

Data Gateway Instance(s) Added to Pool Selected 0 / Filter 0 / Total 2

	In Use	Data Gateway Instance Name	Data Gateway Name
□	No	cdg-az2-156.cisco.com	

Figure 11: Standby Pane for Dual Stack



New York Standby

IPv4 address(s) *

IPv6 address(s) *

FQDN

IPv4 subnet * 16

Range: 1 to 32

IPv4 network gateway *

IPv6 subnet * 64

Range: 1 to 128

IPv6 network gateway *

DG instance types Standard Standard plus with extra resources Extended

Unassigned data gateway instance(s) Selected 0 / Filtered 0 / Total 0

Data gateway instance name	Operational state

Assigned data gateway instance(s) Selected 0 / Filtered 0 / Total 2

	In use	Data gateway instance name	Data gateway name
□	No	coffeecdg4-nyc.cisco.com	
□	No	coffeecdg5-nyc.cisco.com	

Step 5 Click **Create**.

In Amazon EC2, after a pool is created, make sure that the Network Load Balancer is in a healthy state for the active data gateway.

After you click **Save**, a virtual data gateway gets created automatically and is visible under the **Data Gateway instances** tab.

Assign Data Gateways 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 enable the Geo Redundancy capabilities, see the *Enable Geo Redundancy* section in *Cisco Crosswork Network Controller 7.0 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 the 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 allows 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 **NOT_READY**. Crosswork considers this instance as the standby on which the failover happens.
- At least one spare data gateway should be present in both the standby and active cluster, with the status of **NOT_READY**.
- A data gateway in the maintenance mode cannot be used as a spare for the future failover procedures until the administration state as **UP**.

Use these steps 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

In the event of a failover, the primary data gateway (cdg1) switches over to the secondary data gateway (cdg2), and cdg2 takes on the southbound IPv6 address of cdg1. When cdg2 is detected, Crosswork logs an event for cdg2, indicating a Duplicate Address Detection (DAD) failure due to the IP address being a duplicate configuration from dg1. This temporary error occurs while the operating system removes the DAD failed flag from the interface. When the operating system clears the DAD failed status from the interface, the Crosswork Data Gateway switches the gateway to the **UP** state.

If the failover is unsuccessful due to an error, see Data Gateway Failover Failed, on page 97.

Attach Devices to a Crosswork Data Gateway

Before you begin

- Ensure that the **Admin state** and **Operational state** of the data gateway to which you want to attach devices is **Up**.
- The Crosswork Network Controller allows the connection of a device to only one Crosswork Data Gateway at a time.
- For optimal performance, we recommend attaching devices to a Crosswork Data Gateway in batches of 300 devices or fewer.
- Crosswork Data Gateway supports several secure SSH key exchange algorithms. If SSH is failing, make sure your devices are set to use one of these key types:
    - aes128-gcm@openssh.com
    - aes256-gcm@openssh.com
    - aes128-ctr
    - aes192-ctr
    - aes256-ctr
    - blowfish-ctr
    - aes128-cbc
    - aes192-cbc
    - aes256-cbc
    - blowfish-cbc
    - 3des-ctr

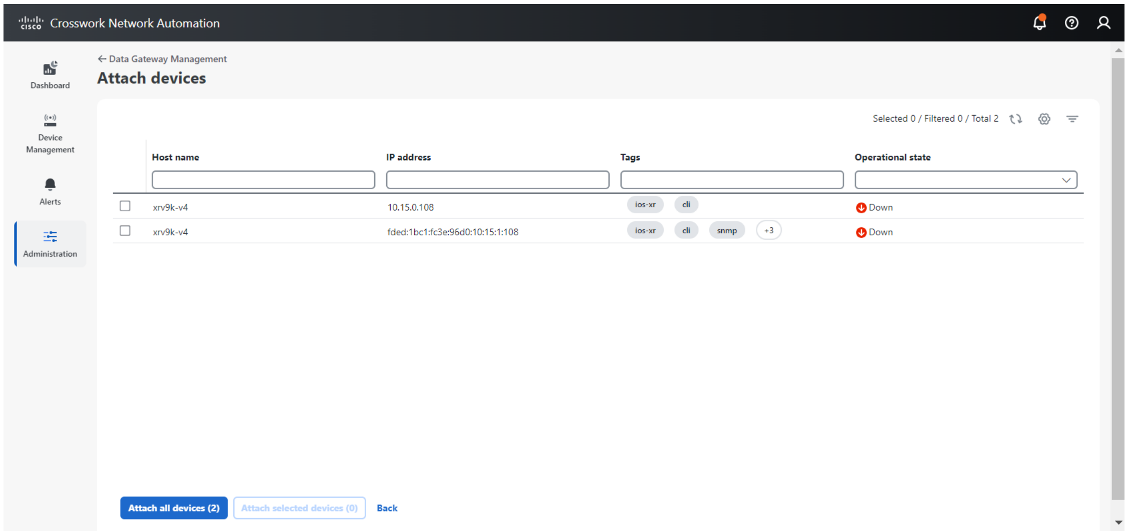
- 3des-cbc
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-96
- hmac-sha1
- hmac-md5-96
- hmac-md5
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512-etm@openssh.com

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 21 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 the **Actions** column, click ··· and select **Attach devices**. The **Attach devices** window opens showing all the devices available for attaching.

Figure 12: Attach Devices Window


Crosswork Network Automation
Dashboard
Device Management
Alerts
Administration
← Data Gateway Management
Attach devices
Selected 0 / Filtered 0 / Total 2
Attach all devices (2)
Attach selected devices (0)
Back

	Host name	IP address	Tags	Operational state
□	xrv9k-v4	10.15.0.108	ios-xr cli	Down
□	xrv9k-v4	fded:1bc1:fc3e:96d0:10:15:1:108	ios-xr cli snmp +3	Down

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 the **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 21.

Manage Crosswork Data Gateway Post-Setup

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

- Monitor Crosswork Data Gateway Health, on page 21
- Edit or Delete a Crosswork Data Gateway Pool, on page 25
- Manage Crosswork Data Gateway Device Assignments, on page 27
- Maintain Crosswork Data Gateway Instances, on page 29

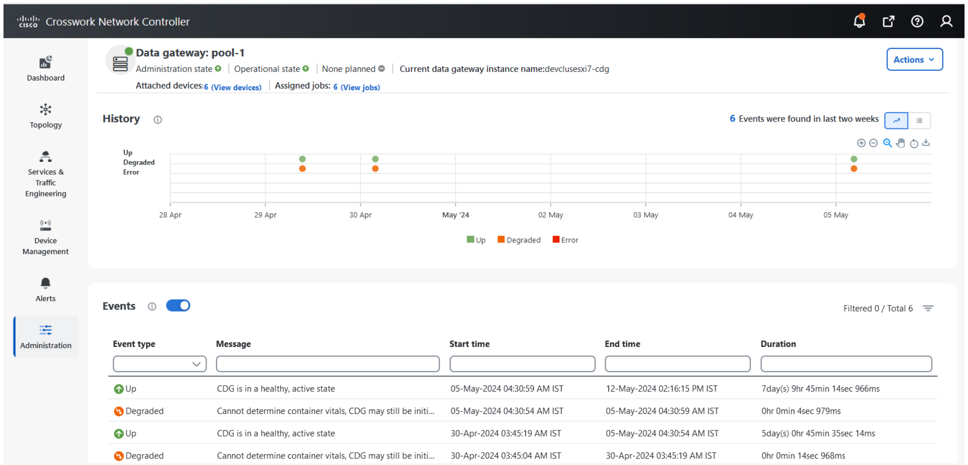
Monitor Crosswork Data Gateway Health

You can view the operations and health summary of a data gateway from the Crosswork Data Gateway vitals page. To access this page, go to **Administration** > **Data Gateway Management** > **Data gateways** and click the pool name in the table. The pool details page opens. This page also has details of the health of various containerized services running on a data gateway. The overall health of a data gateway 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 with a time estimate for the data gateway to reach the destination.
- **Download service metrics**–Downloads the metrics for all collection jobs for a data gateway from the Cisco Crosswork UI.
- **Download showtech**–Downloads the showtech logs from Cisco Crosswork UI.
- **Reboot**–Reboots the data gateway.
- **Change log level**–Allows you to change the log level of a data gateway's components, for example collectors (cli-collector) and infra services (oam-manager). Log level changes apply only to the data gateway on which you are making the change.

Figure 13: Data Gateway Window



Data gateway: pool-1
Administration state | Operational state | None planned | Current data gateway instance name:devclusesxi7-cdg
Attached devices:6 (View devices) | Assigned jobs: 6 (View jobs)

History

6 Events were found in last two weeks

Events

Filtered 0 / Total 6

Event type	Message	Start time	End time	Duration
Up	CDG is in a healthy, active state	05-May-2024 04:30:59 AM IST	12-May-2024 02:16:15 PM IST	7day(s) 9hr 45min 14sec 966ms
Degraded	Cannot determine container vitals, CDG may still be initi...	05-May-2024 04:30:54 AM IST	05-May-2024 04:30:59 AM IST	0hr 0min 4sec 979ms
Up	CDG is in a healthy, active state	30-Apr-2024 03:45:19 AM IST	05-May-2024 04:30:54 AM IST	5day(s) 0hr 45min 35sec 14ms
Degraded	Cannot determine container vitals, CDG may still be initi...	30-Apr-2024 03:45:04 AM IST	30-Apr-2024 03:45:19 AM IST	0hr 0min 14sec 968ms

The following parameters are displayed on this page:

- **General Crosswork Data Gateway details**–Displays general details of 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 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.

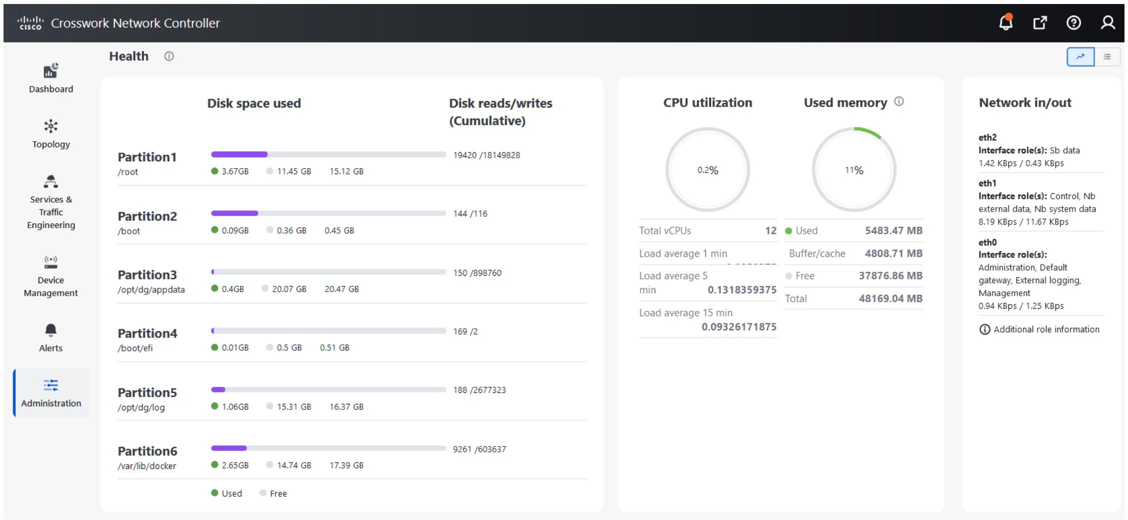
- **Events**–Displays a list of all the data gateway transition state changes over the last 14 days. It includes information such as the event details, including operational state changes, role changes, a message indicating the reason for the status change, timestamp, and duration.

- **Health**–Shows the health information of the data gateways. The timestamp in the top-right corner is the timestamp when the last health data was collected. If the 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 data gateway exceeds 80%, we recommend taking corrective action before the **CPU utilization** increases further leading to failure of the 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 14: Crosswork Data Gateway Health Window



	Disk space used			Disk reads/writes (Cumulative)
Partition1 /root	● 3.67GB	● 11.45 GB	15.12 GB	19420 /18149828
Partition2 /boot	● 0.09GB	● 0.36 GB	0.45 GB	144 /116
Partition3 /opt/dg/appdata	● 0.4GB	● 20.07 GB	20.47 GB	150 /898760
Partition4 /boot/efi	● 0.01GB	● 0.5 GB	0.51 GB	169 /2
Partition5 /opt/dg/log	● 1.06GB	● 15.31 GB	16.37 GB	188 /2677323
Partition6 /var/lib/docker	● 2.65GB	● 14.74 GB	17.39 GB	9261 /603637

● Used ● Free

CPU utilization: 0.2%

Total vCPUs	12
Load average 1 min	
Load average 5 min	0.1318359375
Load average 15 min	0.09326171875

Used memory: 11%

● Used	5483.47 MB
Buffer/cache	4808.71 MB
● Free	37876.86 MB
Total	48169.04 MB

Network in/out

eth2
Interface role(s): Sb data
1.42 KBps / 0.43 KBps

eth1
Interface role(s): Control, Nb external data, Nb system data
8.19 KBps / 11.67 KBps

eth0
Interface role(s): Administration, Default gateway, External logging, Management
0.94 KBps / 1.25 KBps

ⓘ Additional role information

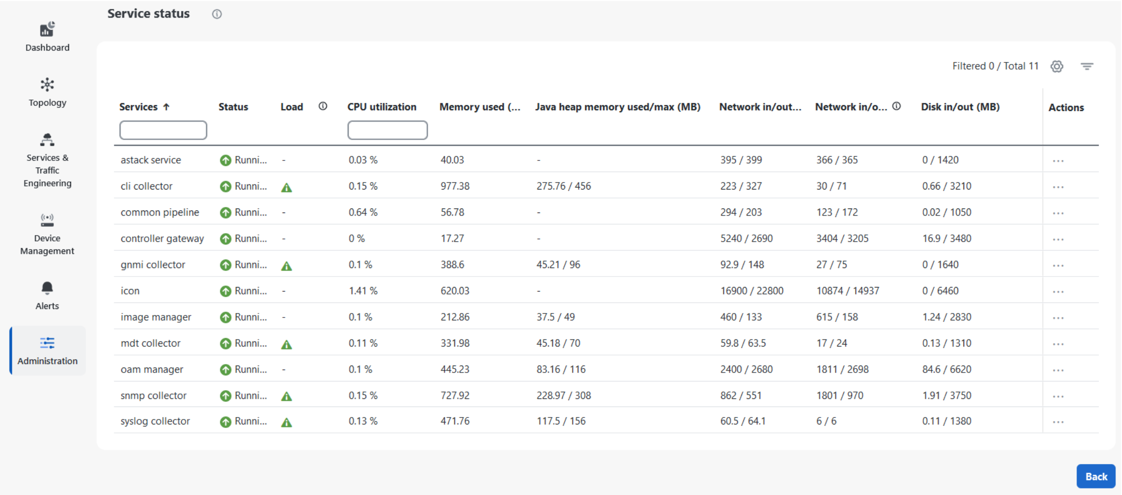
- **Service status**–Displays the health information of the individual container services running on the data gateway and their resource consumption with an option to restart (**Actions** > **Restart**) an individual service. The Load column indicates the processing load of that specific collector/service. 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 15: Service Status Window



Service status

Filtered 0 / Total 11

Services ↑	Status	Load	CPU utilization	Memory used (...	Java heap memory used/max (MB)	Network in/out...	Network in/o...	Disk in/out (MB)	Actions
astack service	Runni...	-	0.03 %	40.03	-	395 / 399	366 / 365	0 / 1420	...
cli collector	Runni...	⚠	0.15 %	977.38	275.76 / 456	223 / 327	30 / 71	0.66 / 3210	...
common pipeline	Runni...	-	0.64 %	56.78	-	294 / 203	123 / 172	0.02 / 1050	...
controller gateway	Runni...	-	0 %	17.27	-	5240 / 2690	3404 / 3205	16.9 / 3480	...
gnmi collector	Runni...	⚠	0.1 %	388.6	45.21 / 96	92.9 / 148	27 / 75	0 / 1640	...
icon	Runni...	-	1.41 %	620.03	-	16900 / 22800	10874 / 14937	0 / 6460	...
image manager	Runni...	-	0.1 %	212.86	37.5 / 49	460 / 133	615 / 158	1.24 / 2830	...
mdt collector	Runni...	⚠	0.11 %	331.98	45.18 / 70	59.8 / 63.5	17 / 24	0.13 / 1310	...
oam manager	Runni...	-	0.1 %	445.23	83.16 / 116	2400 / 2680	1811 / 2698	84.6 / 6620	...
snmp collector	Runni...	⚠	0.15 %	727.92	228.97 / 308	862 / 551	1801 / 970	1.91 / 3750	...
syslog collector	Runni...	⚠	0.13 %	471.76	117.5 / 156	60.5 / 64.1	6 / 6	0.11 / 1380	...

We recommend monitoring the health of the data gateways in your network periodically to prevent overloading and take corrective actions, such as adding more resources or reducing load on the data gateway proactively.

1. The DG-Manager generates alarms when the 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 Viewing Crosswork Data Gateway Alarms, on page 24.

2. If the **CPU utilization** of a 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 data gateway, have added other VMs to the pool, or increase the cadence of existing collection jobs.

3. If the **CPU utilization** of a data gateway exceeds 90%, we recommend that you move devices to another 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 the 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**.

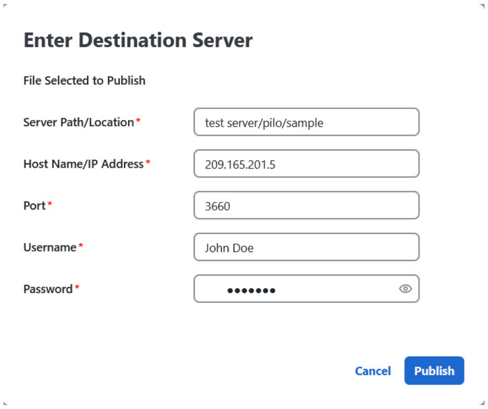
Step 2 In the **Platform Infrastructure** tile, click **View Details**. The **Application Details** window opens.

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 16: Showtech Requests Window



Enter Destination Server

File Selected to Publish

Server Path/Location*	test server/pilo/sample
Host Name/IP Address*	209.165.201.5
Port*	3660
Username*	John Doe
Password*	•••••••

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

Edit or Delete a Crosswork Data Gateway Pool

Follow the steps to edit or delete a data gateway pool. To create a pool, see Create a Data Gateway Pool, on page 10 or Create a Pool in the Geo Redundancy-Enabled Sites, on page 14.

Before you begin

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

- Virtual data gateways or pools that have devices that are 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 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 18.
- Before you delete a data gateway pool, detach devices from the data gateway first or move the devices to another data gateway.

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

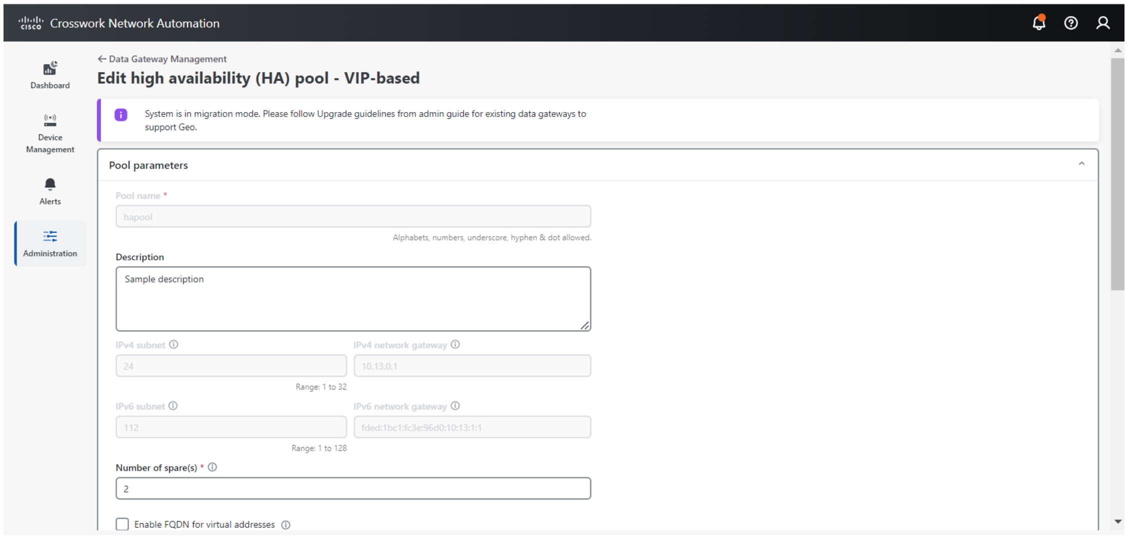
Step 2 **Edit high availability (HA) pool**:

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

b) Click the ✎ button to open the **Edit high availability (HA) pool** page.

When you edit a resource pool, you can only change some of the parameters in the **Pool parameters** pane. To modify the rest of the parameters, create a new pool with the needed values and move the data gateway instances to that pool.

Figure 17: Data Gateway Management - Edit HA Pool Window



Edit high availability (HA) pool - VIP-based

System is in migration mode. Please follow Upgrade guidelines from admin guide for existing data gateways to support Geo.

Pool parameters

Pool name *: hapool
Alphabets, numbers, underscore, hyphen & dot allowed.

Description: Sample description

IPv4 subnet: 24 (Range: 1 to 32)
IPv4 network gateway: 10.13.0.1

IPv6 subnet: 112 (Range: 1 to 128)
IPv6 network gateway: fded:1bc1:fc3e:96d0:10:13:1:1

Number of spare(s) *: 2

☐ Enable FQDN for virtual addresses

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

- Add a virtual IP address or FQDN for every active data gateway needed. For the dual-stack deployment, provide both, IPv4 and IPv6 address.
- Change the number of standby data gateway instances.
- Add and remove data gateway instances from the pool.
- Enable or disable FQDN for the pool.

d) In the **Active** and **Standby** site parameters pane, you can modify the IP or FQDN addresses of the data gateway VM. The Active and Standby panes are visible only when the geo redundancy feature is enabled. For information about the geo redundancy capabilities, see the *Enable Geo Redundancy* section in *Cisco Crosswork Network Controller 7.0 Installation Guide*.

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

Step 3 **Delete a 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 Crosswork Data Gateway Device Assignments

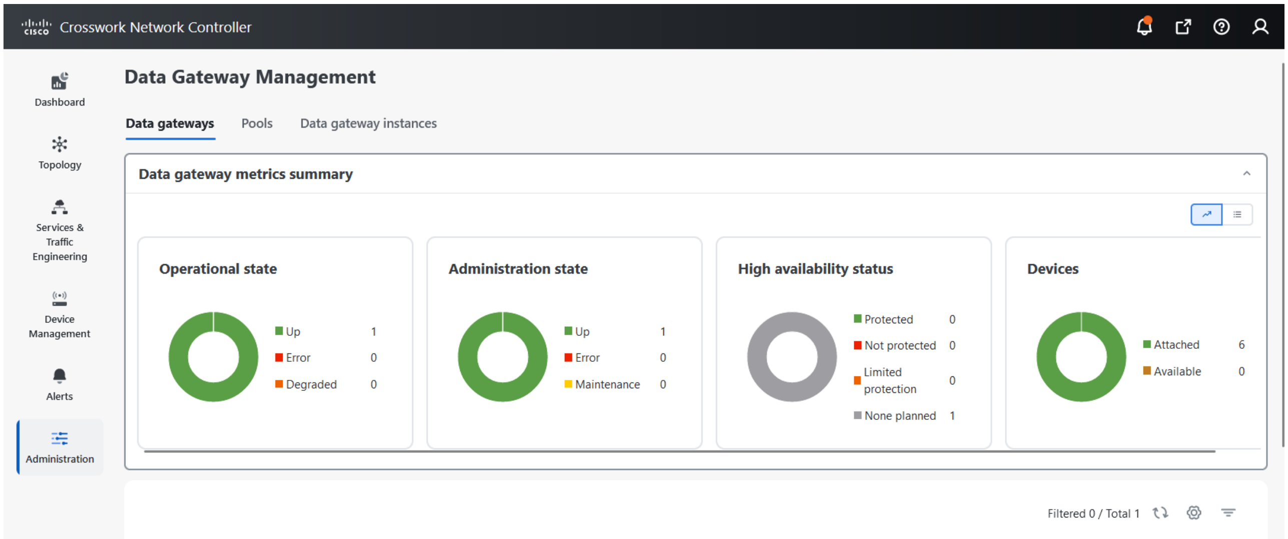
Follow these guidelines when you move or detach devices from a Crosswork Data Gateway.

- A device can be attached to only one Crosswork Data Gateway.
- When moving devices to a Crosswork Data Gateway in a 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 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 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 19.

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

Figure 18: Data Gateways Window

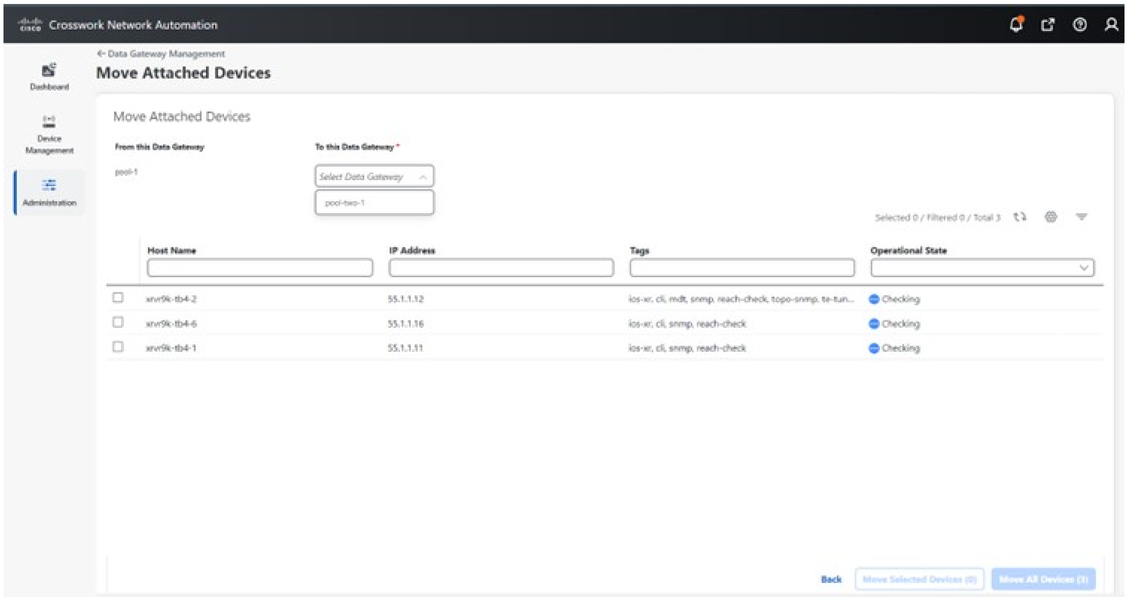


Step 2 **Move Devices**:

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 19: Move Attached Devices Window



← Data Gateway Management

Move Attached Devices

Move Attached Devices

From this Data Gateway: pool-1

To this Data Gateway *: Select Data Gateway — pool-two-1

Selected 0 / Filtered 0 / Total 3

	Host Name	IP Address	Tags	Operational State
□	xrvr9k-tb4-2	55.1.1.12	ios-xr, cli, mdt, snmp, reach-check, topo-snmp, te-tun...	Checking
□	xrvr9k-tb4-6	55.1.1.16	ios-xr, cli, snmp, reach-check	Checking
□	xrvr9k-tb4-1	55.1.1.11	ios-xr, cli, snmp, reach-check	Checking

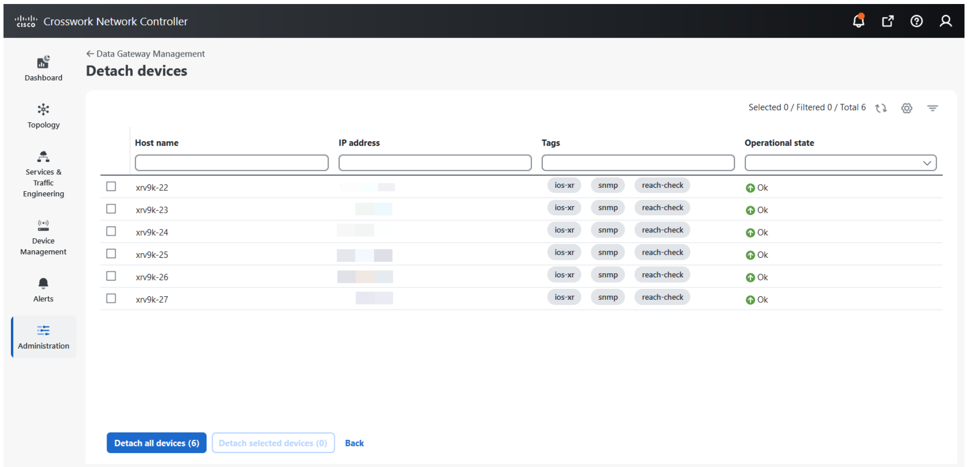
c) To move all the devices, click **Move all devices**. Otherwise, select the devices you want to move and click **Move selected devices**.

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 20: Detach Devices Window



Crosswork Network Controller
Dashboard
Topology
Services & Traffic Engineering
Device Management
Alerts
Administration
Detach all devices (6)
Detach selected devices (0)
Back

← Data Gateway Management

Detach devices

Selected 0 / Filtered 0 / Total 6

	Host name	IP address	Tags	Operational state
□	xrv9k-22	[redacted]	ios-xr snmp reach-check	Ok
□	xrv9k-23	[redacted]	ios-xr snmp reach-check	Ok
□	xrv9k-24	[redacted]	ios-xr snmp reach-check	Ok
□	xrv9k-25	[redacted]	ios-xr snmp reach-check	Ok
□	xrv9k-26	[redacted]	ios-xr snmp reach-check	Ok
□	xrv9k-27	[redacted]	ios-xr snmp reach-check	Ok

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 18.

Maintain Crosswork Data Gateway Instances

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

- Change the Administration State of Crosswork Data Gateway Instance, on page 29
- Delete Crosswork Data Gateway Instance from Crosswork Network Controller, on page 30
- Redeploy a Crosswork Data Gateway Instance, on page 32

Change the Administration State of Crosswork Data Gateway Instance

To perform upgrades or other maintenance within the data center is may become necessary to suspend operations between the Crosswork platform and the Crosswork Data Gateway. This can be done by placing Crosswork Data Gateway into **Maintenance** mode. During downtime, the administrator can modify 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 completed, the admin can change the administration state to **Up**. Once the Crosswork Data Gateway instance is up, Crosswork Network Controller 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 18 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:

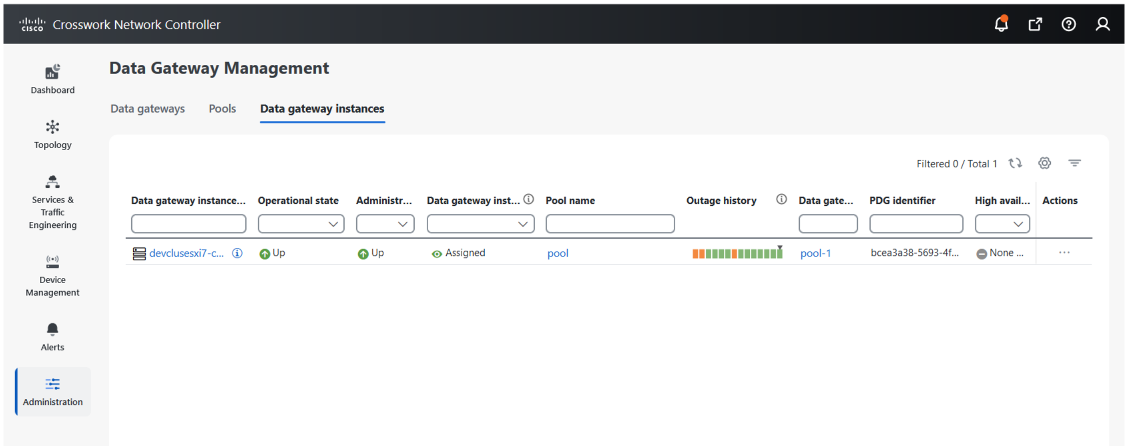
- Spare role when a manual or autofailover occurs.
- Assigned role when it is the only gateway in the pool.

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 the data gateway instance name displays the enrollment details that include interface role details.

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

Figure 21: Data Gateway Instances Window



Data Gateway Management

Filtered 0 / Total 1

Data gateway instance...	Operational state	Administr...	Data gateway inst...	Pool name	Outage history	Data gate...	PDG identifier	High avail...	Actions
devclusesxi7-c... ⓘ	Up	Up	Assigned	pool		pool-1	bcea3a38-5693-4f...	None ...	⋯

Step 3 Select the administration state that you wish to assign to the data gateway instance.

Delete Crosswork Data Gateway Instance from Crosswork Network Controller

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

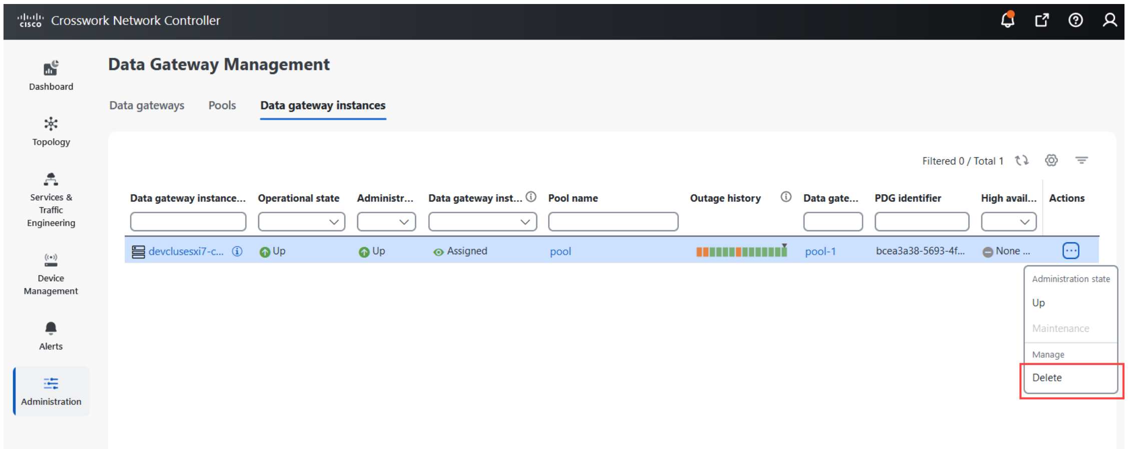
Before you begin

It is recommended that you move the attached devices to another data gateway not to lose any jobs corresponding to these devices. If you detach the devices from 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 the **Actions** column and click **Delete**.

Figure 22: Data Gateway Instances Window

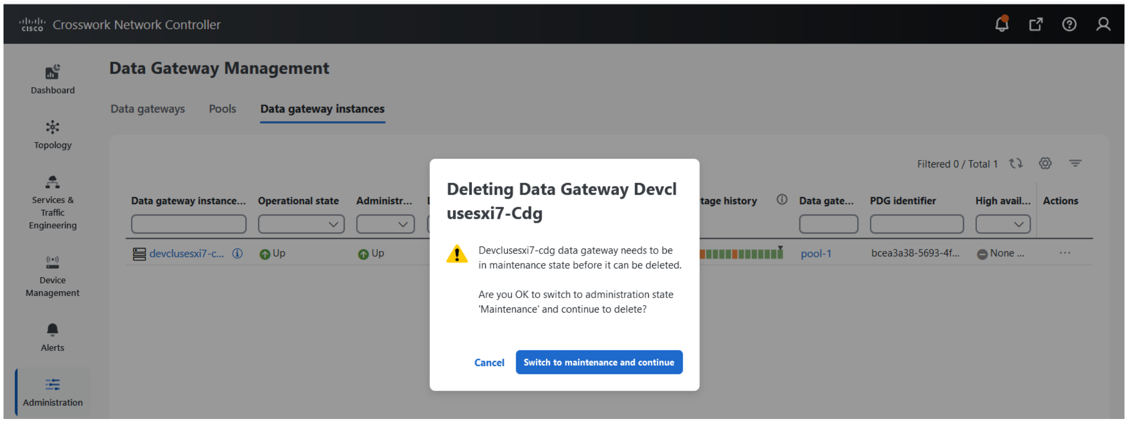


Data gateway instance...	Operational state	Administr...	Data gateway inst...	Pool name	Outage history	Data gate...	PDG identifier	High avail...	Actions
devclusesxi7-c...	Up	Up	Assigned	pool		pool-1	bcea3a38-5693-4f...	None ...	⋯

Step 3

The 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 23: Switch to Maintenance & Continue Pop-up Window



Deleting Data Gateway Devclusesxi7-Cdg

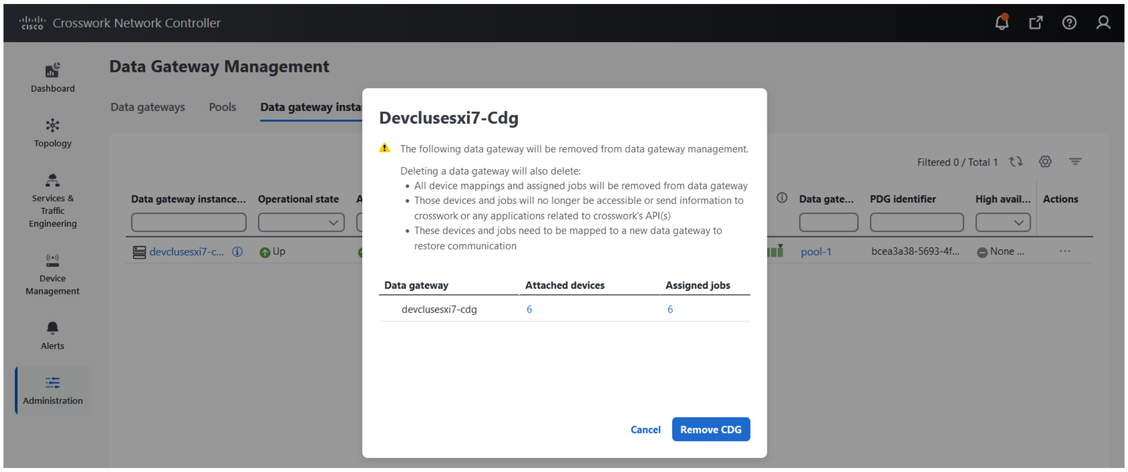
Devclusesxi7-cdg data gateway needs to be in maintenance state before it can be deleted.

Are you OK to switch to administration state 'Maintenance' and continue to delete?

Step 4

Check the check box for **I understand the concern associated with deleting the Data Gateways** and click **Remove CDG**.

Figure 24: Delete Data Gateway Confirmation Dialog Box



Devclusesxi7-Cdg

⚠ The following data gateway will be removed from data gateway management.

Deleting a data gateway will also delete:

- All device mappings and assigned jobs will be removed from data gateway
- Those devices and jobs will no longer be accessible or send information to crosswork or any applications related to crosswork's API(s)
- These devices and jobs need to be mapped to a new data gateway to restore communication

Data gateway	Attached devices	Assigned jobs
devclusesxi7-cdg	6	6

Cancel | Remove CDG

Redeploy a Crosswork Data Gateway Instance

To redeploy a data gateway instance, delete the old instance and install a new one. For details on how to install a new data gateway instance, see *Cisco Crosswork Network Controller 7.0 Installation Guide*.

If you are redeploying the 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 data gateway instance.

Important points to consider

- If the 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 data gateway instance to **Maintenance** for auto-enrollment to go through.
- If a data gateway instance was already enrolled with Cisco Crosswork and Cisco Crosswork was installed again, re-enroll the existing data gateway instance with Cisco Crosswork. See Re-enroll Crosswork Data Gateway.
- If you are redeploying a data gateway instance with the same hostname, clear the existing alarms for that hostname to avoid confusion. Otherwise, the old alarms will still be viewable in the history. With the old alarms, you must check the timestamps. This is necessary to determine whether they were raised on the older data gateway or the current one with the same hostname.

Configure Crosswork Data Gateway Global Settings

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

- Device Packages, on page 40
- Configure Crosswork Data Gateway Global Parameters, on page 44
- Allocate Crosswork Data Gateway Resources, on page 46

Create and Manage External Data Destinations

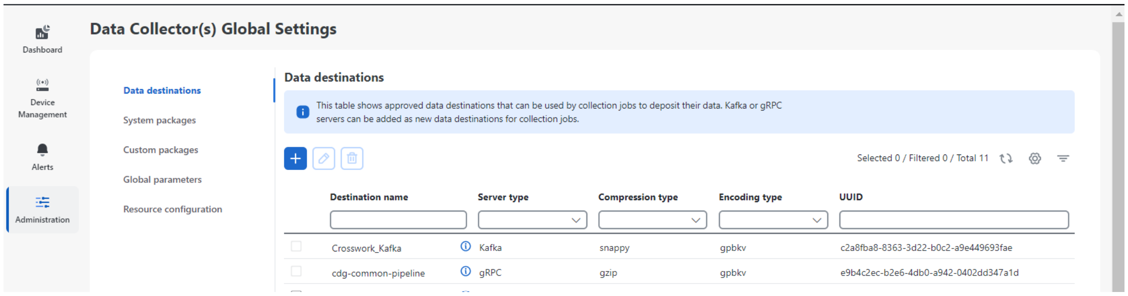
Cisco Crosswork allows you to create external data destinations (Kafka or external gRPC) that can be used by collection jobs to deposit data.

It can be accessed by navigating to **Administration** > **Data Collector(s) 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 25: Data Destinations Window



This table shows approved data destinations that can be used by collection jobs to deposit their data. Kafka or gRPC servers can be added as new data destinations for collection jobs.

	Destination name		Server type	Compression type	Encoding type	UUID
□	Crosswork_Kafka	ⓘ	Kafka	snappy	gpbkv	c2a8fba8-8363-3d22-b0c2-a9e449693fae
□	cdg-common-pipeline	ⓘ	gRPC	gzip	gpbkv	e9b4c2ec-b2e6-4db0-a942-0402dd347a1d

The UUID is the Unique identifier for the data destination. Crosswork Network Controller 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 the 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 Collector(s) 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 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
Server type	From the drop-down, select the server type of your data destination.	Yes	Yes

Field	Value	Available in gRPC	Available in Kafka
Encoding type	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
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

Field	Value	Available in gRPC	Available in Kafka
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 **Destination - Per collector properties** pane:

a) Select a **Collector**.

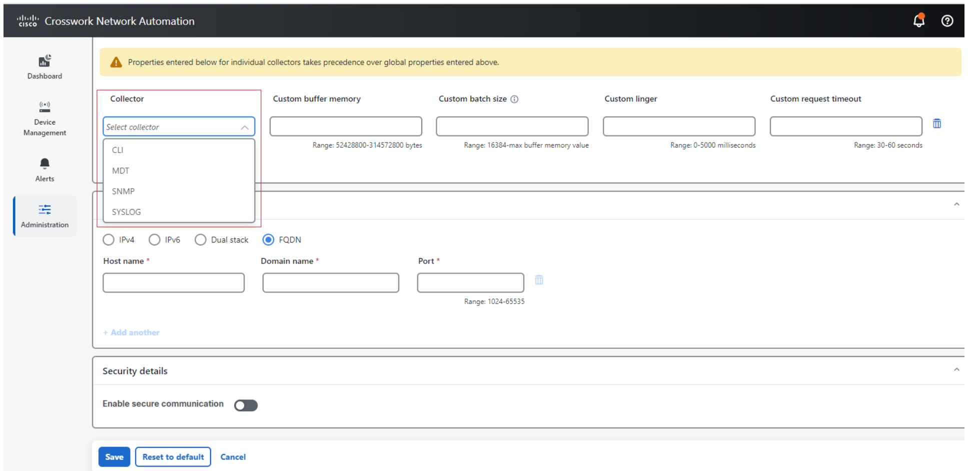
b) Enter values for the following fields:

- **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 26: Add Destination Window



Properties entered below for individual collectors takes precedence over global properties entered above.

Collector: Select collector

Custom buffer memory: Range: 52428800-314572800 bytes

Custom batch size: Range: 16384-max buffer memory value

Custom linger: Range: 0-5000 milliseconds

Custom request timeout: Range: 30-60 seconds

○ IPv4 ○ IPv6 ○ Dual stack ● FQDN

Host name *

Domain name *

Port *: Range: 1024-65535

Security details

Enable secure communication

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, Dual stack, 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.

Note You can modify the port numbers only for user-defined destinations and not for system-created destinations.

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**. IPv4 subnet mask ranges from 1 to 32 and port range from 1024 to 65535. IPv6 subnet mask ranges from 1 to 128 and port range from 1024 to 65535.	Yes	Yes

Connectivity Type	Fields	Available in gRPC	Available in Kafka
Dual Stack	Enter the **IPv4 address/ Subnet mask**, **IPv6 address/ Subnet mask**, and **Port**. You can add multiple addresses by clicking **+ Add another**.	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 nnother**.	Yes	Yes

If the IP and port (or FQDN and port) connectivity details match an existing destination, you'll be prompted with a confirmation message for creating a duplicate destination.

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. When the destination is in an error state, the collection job status will be degraded.

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.

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. Suppose the default package that Crosswork provides does not suit your environment, such as if you need to collect data from a third-party device or want specific data that the default MIB package does not support. In that case, customize the package and upload it to Crosswork. For assistance with the customization of the package, contact Cisco or your Cisco partner.

Custom Packages

You can upload the following 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. However, you can use the aggregate package if you want to bundle different files for different devices in a single package.

2. **Custom MIB package**: 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 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**: 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.

4. **Aggregate package**: The aggregate package option allows you to include multiple supported file extensions in a single package. These files can be collector and application-specific files. For instance, an aggregate package can consist of files for CLI and SNMP device packages.

   In the Crosswork UI, you can upload or download these packages. Each package may contain one or multiple files with the following extensions:

   Collector files:

- YANG (.yang)
- MIB (.mib, .my)
- Definition (.def)
- Device Packages (.xar)

Application files:

- Device-metadata (.yaml, .yml)
- Zips (.zip)
- SDU bundle (.sdu)

Workflow for Adding a Custom Package

Use this workflow to learn how to add a custom package for non-Cisco devices.

1. Obtain the YANG model files for the devices you want to support from the vendors.
2. Store the files in a `common/` directory.
3. Create a single custom package by tarring up the directory.
4. Load or add that file to Crosswork Network Controller.

Note Crosswork Network Controller can only load one file at a time. If you have loaded a package with two files and need to add support for a third type of device, add the file in the common directory and then create a replacement file with all three files to upload.

Add Custom Packages

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

1. To update a custom CLI device package, click the upload icon next to the file name on the **Custom packages** page. Updating a custom package means that the existing file will be replaced.
2. To upload multiple xar files, you can bundle them into a single tar.gz package.
3. Crosswork Network Controller doesn't allow Custom MIB package files to overwrite the System MIB Package files. It results in a failed upload attempt.
4. Ensure that the custom package TAR file has only the package folders and none of the parent folders or hierarchy of folders as part of the TAR file. If not imported properly, Crosswork Network Controller throws exceptions when executing the job with a custom package.

Note Crosswork Network Controller 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 the Custom MIB Package, ensure that those new MIBs files can be uploaded within collectors along with the existing System MIB files that are, all dependencies in the files are resolved properly.
- If you plan on adding an Aggregate package, ensure that:
    - The package must contain only supported file extensions. For a list of supported extensions, refer to Custom Packages, on page 40.
    - The files must only be bundled in the .tar.gz format.
    - The top-level directory must contain at least one of the specified collector types:
        - snmp
        - cli
        - common

Sample directory structure:

```
├── cli
│   ├── defs
│   │   └── cli-def1.def
│   ├── device-metadata
│   │   ├── cli.yml
│   │   └── cli-device-metadata.yaml
│   ├── zips
│   │   └── cli-zip.zip
│   ├── sdus
|   │   └── cli-sdu.sdu
│   ├── xars
│   │   ├── cli-xar1.xar
│   │   └── cli-xar2.xar
│   └── yangs
│       ├── cli-yang1.yang
│       └── cli-yang2.yang
├── common
│   ├── defs
│   │   └── common-def1.def
│   ├── device-metadata
│   │   ├── common.yml
│   │   └── common-device-metadata.yaml
│   ├── zips
│   │   └── common-zip.zip
│   ├── mibs
│   │   ├── common-mib1.mib
│   │   └── common-mib2.my
│   ├── sdus
|   │   └── common-sdu.sdu
│   ├── xars
│   │   ├── common-xar1.xar
│   │   └── common-xar2.xar
│   └── yangs
│       ├── common-yang1.yang
│       └── common-yang2.yang
└── snmp
    ├── defs
    │   └── snmp-def1.def
    ├── device-metadata
```

```
│   ├── snmp.yml
│   └── snmp-device-metadata.yaml
├── mibs
│   ├── snmp-mib1.mib
│   └── snmp-mib2.my
├── sdus
│   └── snmp-sdu.sdu
├── zips
│   └── snmp-zip.zip
├── xars
│   ├── snmp-xar1.xar
│   └── snmp-xar2.xar
└── yangs
    ├── snmp-yang1.yang
    └── snmp-yang2.yang
```

- When you upload the aggregate package, the files located in the `cli/` and `snmp/` directories is accessible to the CLI and SNMP collectors. Also, the files in the `common/` directory is accessible to both the CLI and SNMP.

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 are, to check if they can be uploaded to Crosswork Network Controller, see Use Custom MIBs and Yangs on Cisco DevNet.

Step 1 From the main menu, choose **Administration** > **Data Collector(s) Global Settings** > **Custom packages**.

Step 2 In the **Custom packages** page, click +.

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. We recommend including a unique description for each package to easily distinguish between them.

Step 6 Click **Upload**.

What to do next

Restart all the 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 Collector(s) Global Settings** > **Custom packages**.

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.

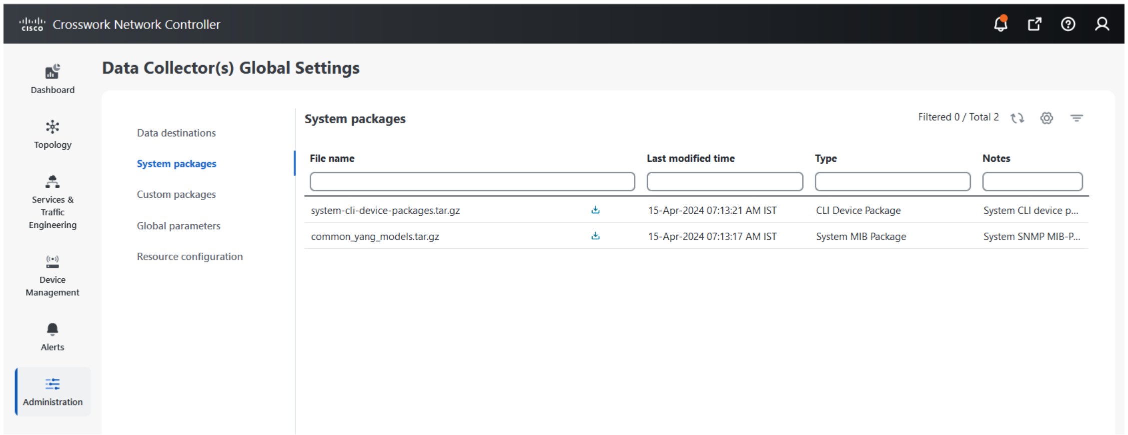
System Device Package

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 27: System Device Packages Window



Data Collector(s) Global Settings

System packages

File name	Last modified time	Type	Notes
system-cli-device-packages.tar.gz ⭳	15-Apr-2024 07:13:21 AM IST	CLI Device Package	System CLI device p...
common_yang_models.tar.gz ⭳	15-Apr-2024 07:13:17 AM IST	System MIB Package	System SNMP MIB-P...

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

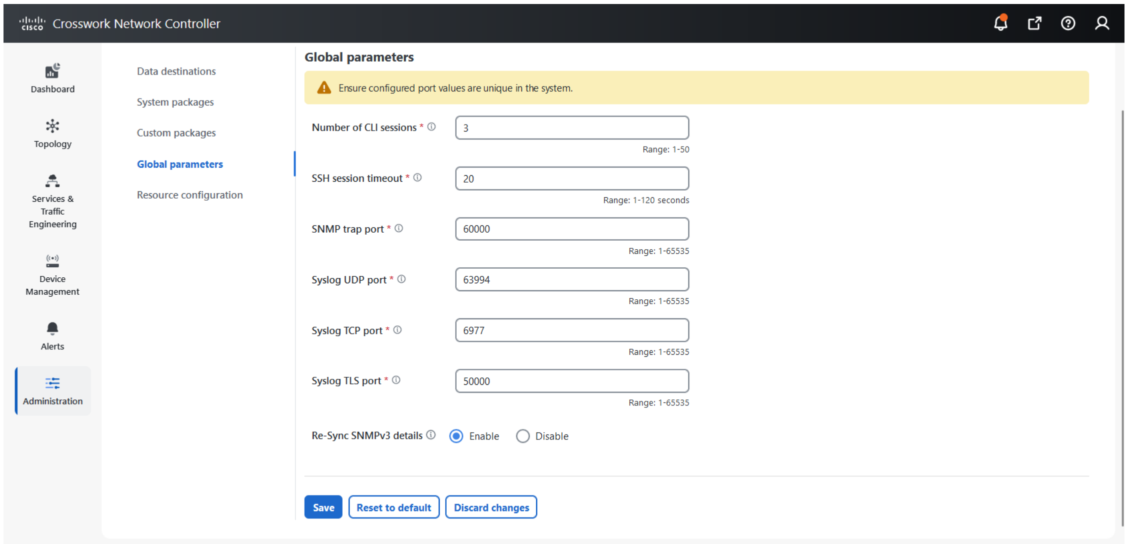
Configure Crosswork Data Gateway Global Parameters

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 Collector(s) Global Settings** > **Global parameters** .

Figure 28: Global Parameters Window



Global parameters

Ensure configured port values are unique in the system.

Number of CLI sessions * 3 (Range: 1-50)

SSH session timeout * 20 (Range: 1-120 seconds)

SNMP trap port * 60000 (Range: 1-65535)

Syslog UDP port * 63994 (Range: 1-65535)

Syslog TCP port * 6977 (Range: 1-65535)

Syslog TLS port * 50000 (Range: 1-65535)

Re-Sync SNMPv3 details ● Enable ○ Disable

Step 2 Change one or more of the global parameters as needed.

To properly update port values, you should:

- Confirm that the port values you want to update are valid ports.
- Verify that the new port values do not conflict with existing port values that are configured on Crosswork Data Gateway.
- Configure the same port values on the device.

Parameter Name	Description	Default value for cluster VM deployment
Number of CLI sessions	Maximum number of CLI sessions between a Crosswork Data Gateway and devices. **Note** This value overrides any internal configuration set for the same parameter.	3 Accepted range is 1-50
SSH session timeout	The session timeout (in seconds) is the duration for which a CLI connection can remain idle in the CLI and SNMP collectors.	120 Accepted range is 1-120 seconds
SNMP trap port	Modify the value as per your deployment environment and configuration requirements.	1062 Accepted range is 1–65535
Syslog UDP port	Modify the value as per your deployment environment and configuration requirements.	9514 Accepted range is 1–65535
Syslog TCP port	-	9898 Accepted range is 1–65535

Parameter Name	Description	Default value for cluster VM deployment
Syslog TLS port	-	6514 Accepted range is 1–65535
Re-Sync SNMPv3 details	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 first collection failure.	Disable

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 the 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 the **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 that is currently configured for collector services are displayed on this page. Any changes that you make to the memory values applies to the currently enrolled and future Crosswork Data Gateways.

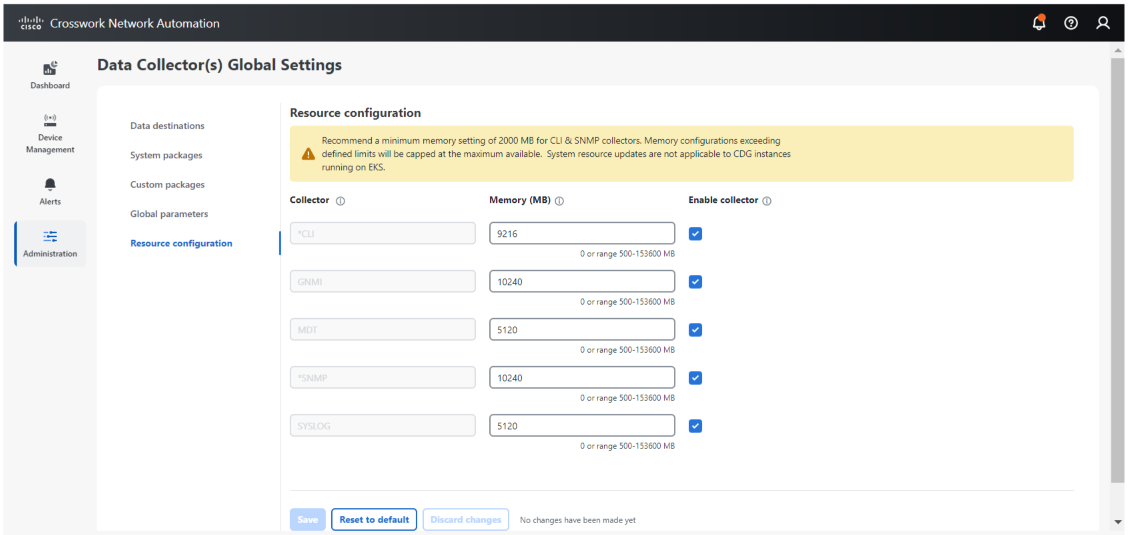
Note The list of collectors that is displayed on this page is dynamic, that is, it is specific to the deployment.

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 29: Resource Configuration Window



Data Collector(s) Global Settings

Resource configuration

Recommend a minimum memory setting of 2000 MB for CLI & SNMP collectors. Memory configurations exceeding defined limits will be capped at the maximum available. System resource updates are not applicable to CDG instances running on EKS.

Collector	Memory (MB)	Enable collector
*CLI	9216 0 or range 500-153600 MB	☑
GNMI	10240 0 or range 500-153600 MB	☑
MDT	5120 0 or range 500-153600 MB	☑
*SNMP	10240 0 or range 500-153600 MB	☑
SYSLOG	5120 0 or range 500-153600 MB	☑

No changes have been made yet

Note The NETCONF data collection support is deprecated starting from the Crosswork Network Controller 6.0 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 collectors.

Step 3 Select the **Enable collector** check box to enable the data collection for the corresponding collector.

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:

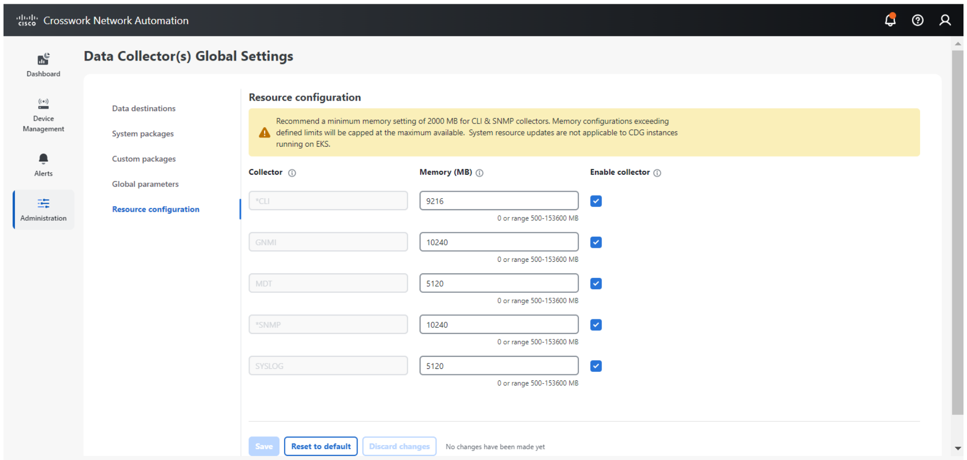
- The data collection for the SNMP and CLI collectors (containers) cannot be disabled. These collectors are required to check the device reachability.
- By default, the collectors are in the enabled state.

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 Collector(s) Global Settings** > **Resource configuration**.

The list of collectors and the resource limits is displayed.

Figure 30: Enabling or Disabling Collectors



Data Collector(s) Global Settings

Resource configuration

Recommend a minimum memory setting of 2000 MB for CLI & SNMP collectors. Memory configurations exceeding defined limits will be capped at the maximum available. System resource updates are not applicable to CDG instances running on EKS.

Collector	Memory (MB)	Enable collector
*CLI	9216 0 or range 500-153600 MB	☑
GNMI	10240 0 or range 500-153600 MB	☑
MDT	5120 0 or range 500-153600 MB	☑
*SNMP	10240 0 or range 500-153600 MB	☑
SYSLOG	5120 0 or range 500-153600 MB	☑

No changes have been made yet

Note The NETCONF data collection support is deprecated starting from the Crosswork Network Controller 6.0 release.

Step 2 Select the **Enable collector** check box to enable the data collection for the corresponding collector. To disable the data collection, ensure to deselect the check box.

Step 3 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.

Crosswork Data Gateway Collection Jobs

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

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

Note The NETCONF data collection support is deprecated starting from the Crosswork Network Controller 6.0 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 Crosswork. Cisco Crosswork creates system jobs for this purpose. If you want the data gateway to collect specific information from non-Cisco devices, you must use custom device packages. For more information on custom device packages, see Custom Packages, on page 40.

   To learn how to build a model that enables an Crosswork to communicate with non-Crosswork devices, see Cisco Devnet.

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 33.

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 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).

You can view collection jobs currently active on all the data gateway instances enrolled with Crosswork Network Controller 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. The **Parametrized Jobs** pane lists all active CLI and gNMI jobs that are created by the Service Health application.

For more information, see Monitor Collection Jobs, on page 86.

Types of Collection Jobs

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

- CLI Collection Job, on page 50
- SNMP Collection Job, on page 51
- MDT Collection Job, on page 59
- Syslog Collection Job, on page 61
- gNMI Collection Job, on page 70

For each collection job that you create, Crosswork Data Gateway executes the collection request and forwards the collected data to the specified 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 Crosswork UI is Unknown. Upon receiving a collection job, 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 **Cadence** value determines the frequency at which data gateway collects the data from the device. You can set the frequency between 10 and 604800000 milliseconds. We recommend a cadence of minimum 60 milliseconds.

When setting the cadence, consider how often the data in the device is subject to change and if the data is operationally significant. We recommend a higher cadence for consistent data like memory consumption or CPU utilization. For more dynamic data points, set a shorter cadence. If the data gateway has to collect a lot of telemetry and more extensive data sets with a short cadence, there is an extra load on the devices and Crosswork Network Controller. As it is difficult to model these loads, we recommend tha you experiment to find the values that provide the best operational insight and, most importantly, actionable information.

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

CLI Collection Job

Crosswork Data Gateway supports CLI-based data collection from the network devices using these commands:

- `show` and the short version `sh`
- `traceroute`
- `dir`

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

You can create a CLI collection job from the Cisco Crosswork UI or using APIs. For information on creating a job from the UI, see Create a Collection Job from Cisco Crosswork UI, on page 81 and from the API, see Cisco DevNet.

Sample Payload of CLI Collection API

This 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 must 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": "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

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

The SNMP collector makes a poll request to Crosswork Network Controller 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 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. You can create the SNMP OID-based collection jobs from the Cisco Crosswork UI or using the API, and SNMP-traps using the API.

The device packages can be imported into the Crosswork Data Gateway instance as described in Section Add Custom Packages, on page 41.

Supported SNMP versions for data polling and traps are:

- Polling Data
  - SNMPv2
  - SNMPv3 (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
  - SNMPv2
  - SNMPv3 (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, 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 User Interface.

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": "YmNjZjEzMTktZjFlOS00NTE5LWI4OTgtY2Y1ZmQxZDFjNWExOlRSQVBfQ09MTEVDVE9S",
  "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, Crosswork Network Controller does not replay the jobs for config update on the devices as this involves NSO. You have to restore configs on NSO/devices. Crosswork Network Controller 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 are sent. For sample device configuration, see Configure Non-secure Syslog on Device, on page 65. 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 67.

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. The 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 Crosswork Network Controller 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.

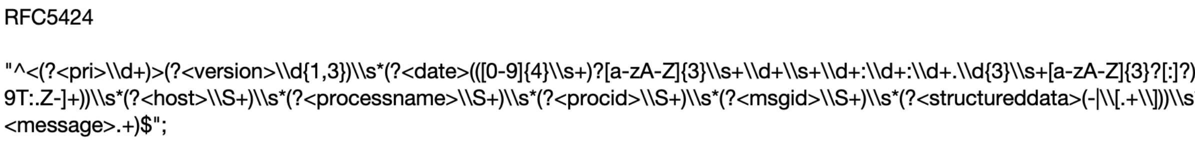
   Note If the device is configured to generate syslog events in RFC5424/RFC3164 format but no format is specified in the **Syslog Format** field, this is considered as **UNKNOWN** by default.

   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 Non-secure Syslog on Device

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

In a dual-stack Crosswork deployment, to make sure that syslog events are logged without interruption, the device must send the events using the same IP stack (either IPv4 or IPv6) that's configured in the device inventory. We recommend that you set the data gateway host address as IP address (IPv4 or IPv6) instead of

FQDN. This ensures that the device's source IP in the events sent to the data gateway matches the device's configuration in the device inventory.

Note The syslog format that you configure for the device must match the format that you specified when the device was added through the Crosswork UI. See Add Devices Through the User Interface for more information.

Configure RFC3164 Syslog format

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

For IOS XR:

```
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 IOS XE:

```
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 IOS XR:

```
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 IOS XE:

```
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
```

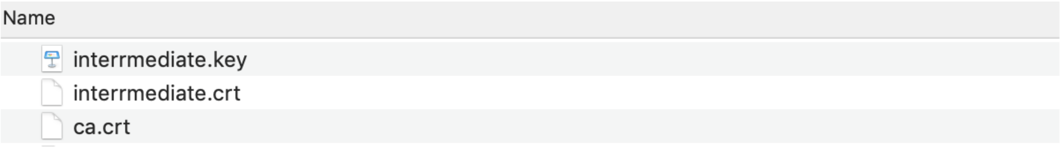
Configure Secure Syslog on Device

In a dual-stack Crosswork deployment, to make sure that syslog events are logged without interruption, the device must send the events using the same IP stack (either IPv4 or IPv6) that's configured in the device inventory. If the data gateway host address is set to FQDN on the device and it resolves to both IPv4 and IPv6, ensure that the device's source IP in the events sent to the data gateway matches the device's configuration in the device inventory.

Use the steps to establish a secured syslog communication with the device.

1. Download the Cisco Crosswork trust chain from the **Certificate Management UI** page in Cisco Crosswork.
   a. In the Cisco Crosswork UI, go to **Administration** > **Certificate Management**.
   b. Click *i* in the **crosswork-device-syslog** row.
   c. Click **Export All** to download the certificates.

      The following files are downloaded to your system.



Name
interrmediate.key
interrmediate.crt
ca.crt

2. Configure the device with the Cisco Crosswork trustchain.

   Refer to the sample configurations to enable Cisco Crosswork Trustpoint on device.

Sample IOS 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 VIP FQDN name>
!
logging trap debugging
logging format rfc5424
logging facility user
logging hostnameprefix ASR9k
logging suppress duplicates

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

Sample IOS 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

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

a. Configure the domain name and DNS IP on the device.

For IOS XR:

```
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>
```

For IOS XE:

```
Device(config)# ip name-server <IP of DNS>
Device(config)# ip domain name <domain name>
```

b. Configure Crosswork Data Gateway VIP FQDN for `tls-hostname`.

For IOS XR:

```
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>
```

For IOS XE:

```
Device(config)# logging host fqdn ipv4 <hostname> transport tls port 6514
```

gNMI Collection Job

Crosswork Network Controller supports gRPC Network Management Interface (gNMI) based telemetry data collection via 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 Device Configuration for gNMI, on page 78.

In gNMI, both secure and insecure mode can co-exist on the device. Crosswork Network Controller 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.

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
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 74.

2. Upload the certificates to the Crosswork Certificate Management UI in Cisco Crosswork. See Configure gNMI Certificate, on page 75.
3. Update device configuration with secure gNMI port details from Cisco Crosswork UI. See Update Protocol on Device from Cisco Crosswork, on page 78.
4. Enable gNMI on the device. See Device Configuration for gNMI, on page 78.
5. Enable gNMI bundling on the device. See Configuring gNMI Bundling for IOS XR, on page 80.
6. Configure the certificates and device key on the device. See Import and Install Certificates on Devices, on page 76.

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.

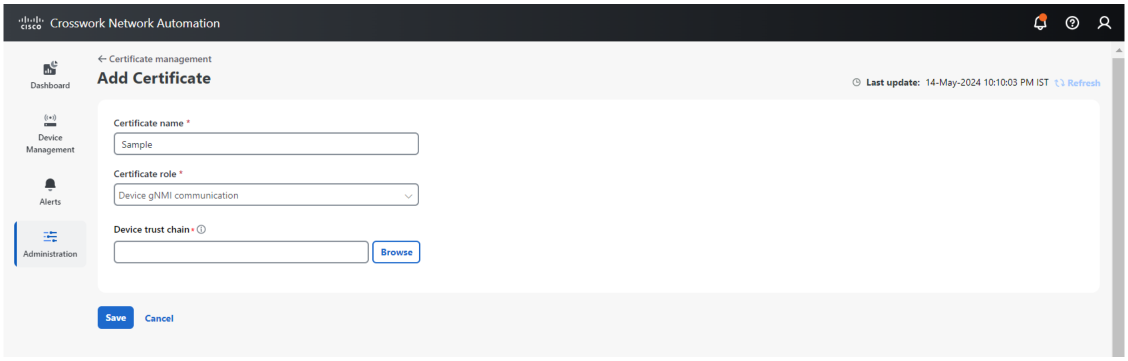
Step 1 From the Cisco Crosswork UI, go to **Administration** > **Certificate Management**.

Step 2 Click the + icon to add the certificate.

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

- **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 31: Add Certificate Window



Add Certificate

Last update: 14-May-2024 10:10:03 PM IST Refresh

Certificate name *: Sample

Certificate role *: Device gNMI communication

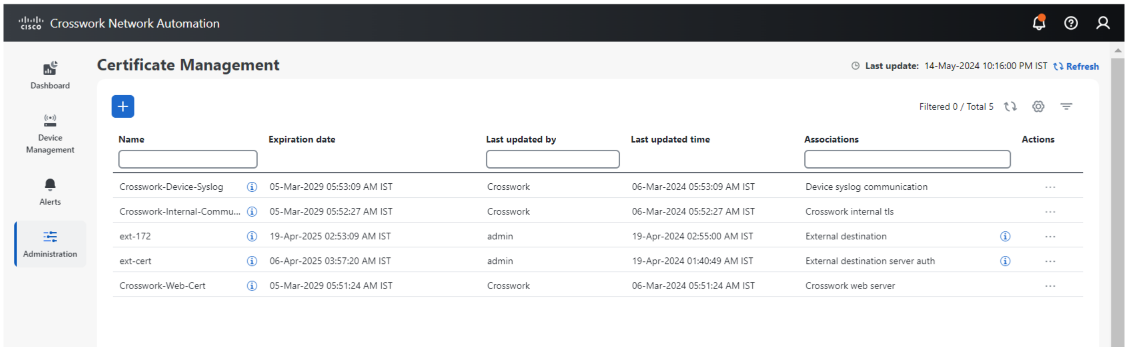
Device trust chain *:

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 32: Certificates Management Window



Certificate Management

Last update: 14-May-2024 10:16:00 PM IST Refresh

Filtered 0 / Total 5

Name	Expiration date	Last updated by	Last updated time	Associations	Actions
Crosswork-Device-Syslog	05-Mar-2029 05:53:09 AM IST	Crosswork	06-Mar-2024 05:53:09 AM IST	Device syslog communication	···
Crosswork-Internal-Commu...	05-Mar-2029 05:52:27 AM IST	Crosswork	06-Mar-2024 05:52:27 AM IST	Crosswork internal tls	···
ext-172	19-Apr-2025 02:53:09 AM IST	admin	19-Apr-2024 02:55:00 AM IST	External destination	···
ext-cert	06-Apr-2025 03:57:20 AM IST	admin	19-Apr-2024 01:40:49 AM IST	External destination server auth	···
Crosswork-Web-Cert	05-Mar-2029 05:51:24 AM IST	Crosswork	06-Mar-2024 05:51:24 AM IST	Crosswork web server	···

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-----
```

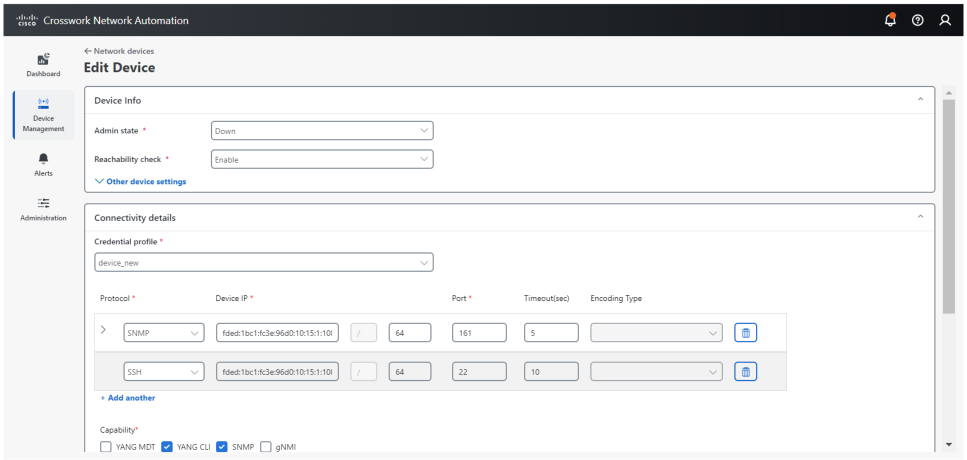
```
quit

# 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 33: Edit Device Details Window



Edit Device

Device Info

Admin state *: Down

Reachability check *: Enable

Other device settings

Connectivity details

Credential profile *: device_new

Protocol *	Device IP *			Port *	Timeout(sec)	Encoding Type
SNMP	fded:1bc1:fc3e:96d0:10:15:1:10ł	/	64	161	5	
SSH	fded:1bc1:fc3e:96d0:10:15:1:10ł	/	64	22	10	

+ Add another

Capability*

□ YANG MDT ☑ YANG CLI ☑ SNMP □ gNMI

Device Configuration for gNMI

This section describes the steps to configure the IOS XR and IOS XE devices to support gNMI-based telemetry data collection.

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 57344–57999. 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 the server vrf.

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

```
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 insecure mode:

```
Device# configure terminal
Device(config)# gnmi-yang
Device(config)# gnmi-yang server
Device(config)# gnmi-yang port 50000 <The default port is 50052.>
Device(config)# end
Device
```

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

```
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 50001 <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 Crosswork Network Controller UI page can only be published once.

Before you begin

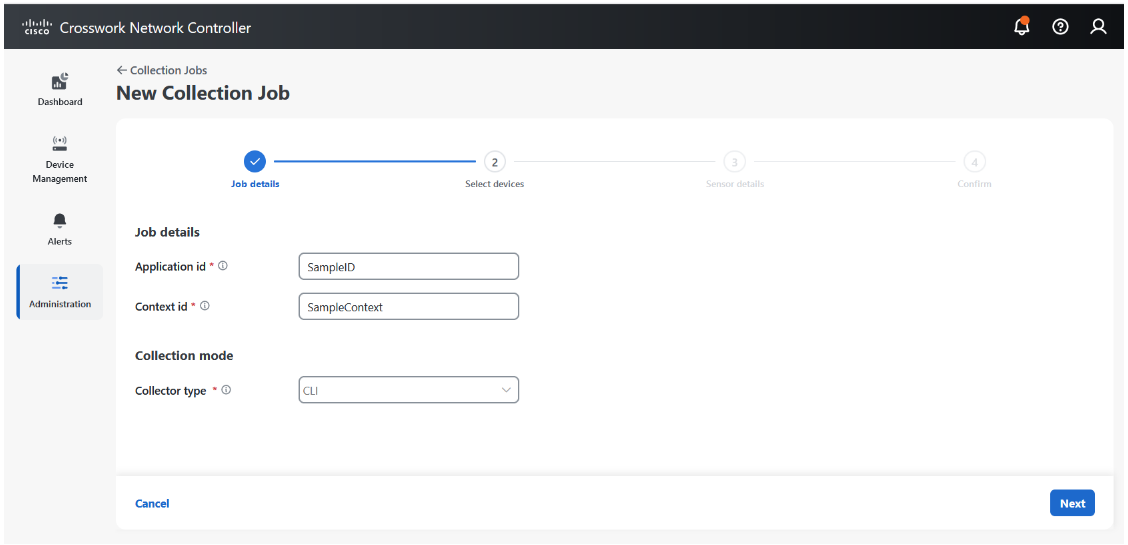
Ensure that a data destination is created (and active) to deposit the collected data. Also, have details of the sensor path and MIB that you plan to collect data from.

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

Step 2 In the left pane, click the + button.

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

Figure 34: New Collection Job Window



Job details

Application id * SampleID

Context id * SampleContext

Collection mode

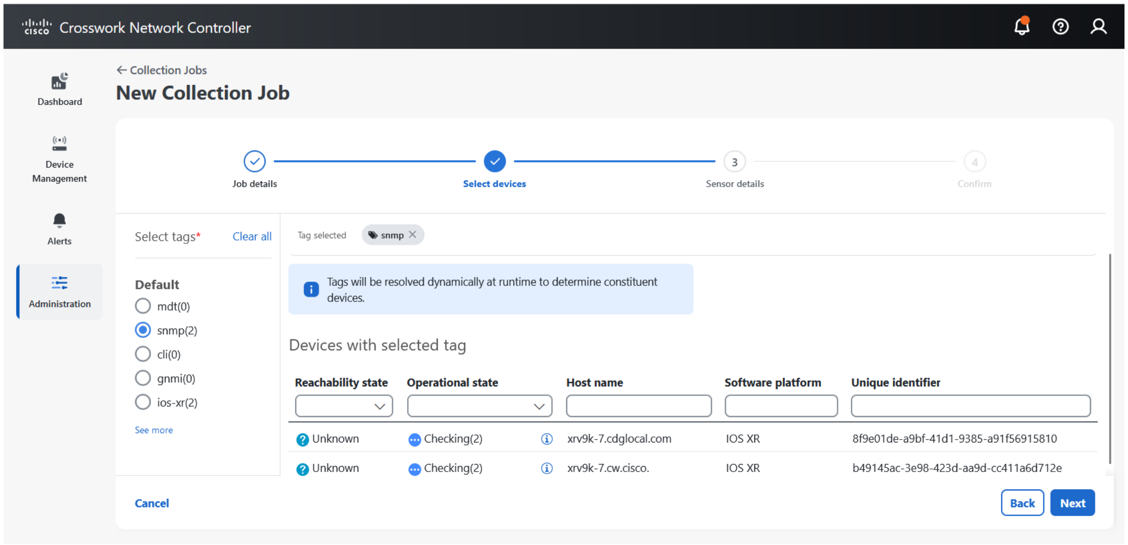
Collector type * CLI

- Application Id: A unique identifier for the application.
- Context Id: 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 the device tag or manually. Click **Next**.

Figure 35: Select Devices Window



New Collection Job

Select tags*

Tag selected: snmp ✕

Default
- ○ mdt(0)
- ● snmp(2)
- ○ cli(0)
- ○ gnmi(0)
- ○ ios-xr(2)

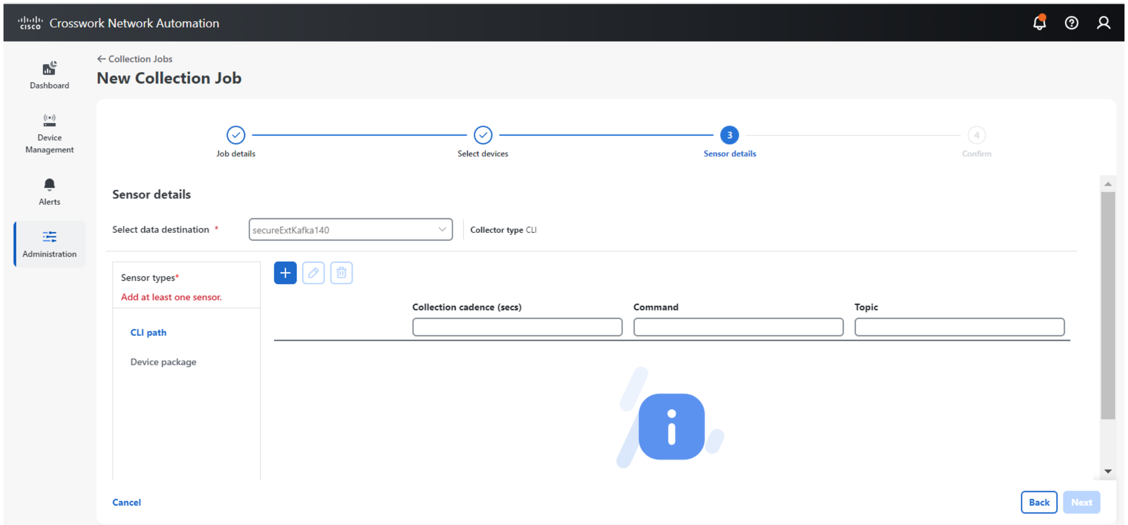
Tags will be resolved dynamically at runtime to determine constituent devices.

Devices with selected tag

Reachability state	Operational state	Host name	Software platform	Unique identifier
Unknown	Checking(2)	xrv9k-7.cdglocal.com	IOS XR	8f9e01de-a9bf-41d1-9385-a91f56915810
Unknown	Checking(2)	xrv9k-7.cw.cisco.	IOS XR	b49145ac-3e98-423d-aa9d-cc411a6d712e

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

Figure 36: Sensor Details Window for CLI Path



New Collection Job

Sensor details

Select data destination *: secureExtKafka140

Collector type CLI

Sensor types*

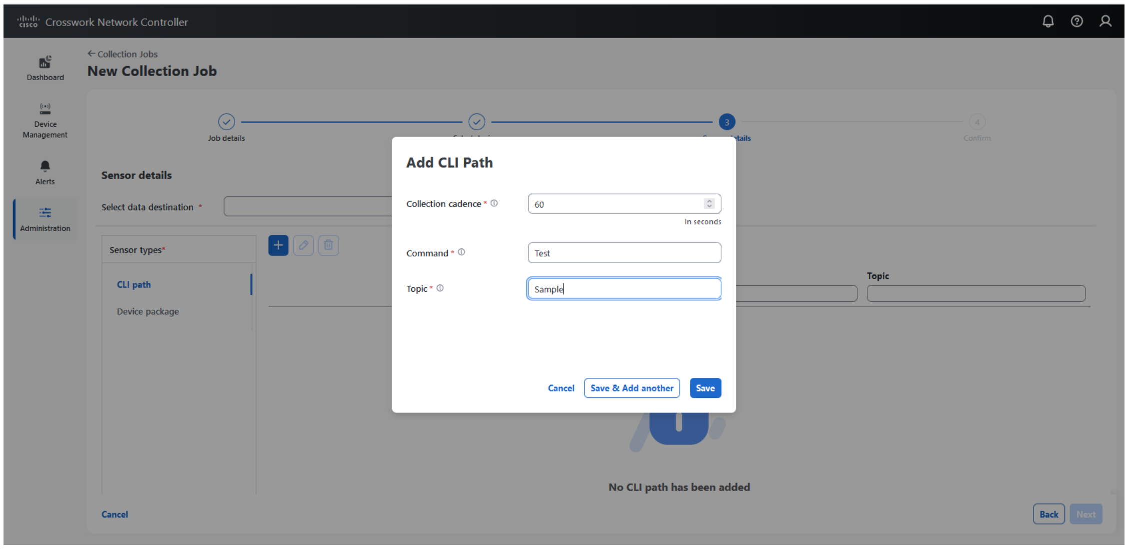
Add at least one sensor.

Collection cadence (secs)	Command	Topic

- Select a data destination from the **Select data destination** drop-down list.
- Select the sensor type from the **Sensor types** pane on the left.

If you selected **CLI path**, Click the + button and enter the following parameters in the **Add CLI Path** dialog box.

Figure 37: Add CLI Path Dialog Box



Add CLI Path

Collection cadence * 60 (In seconds)

Command * Test

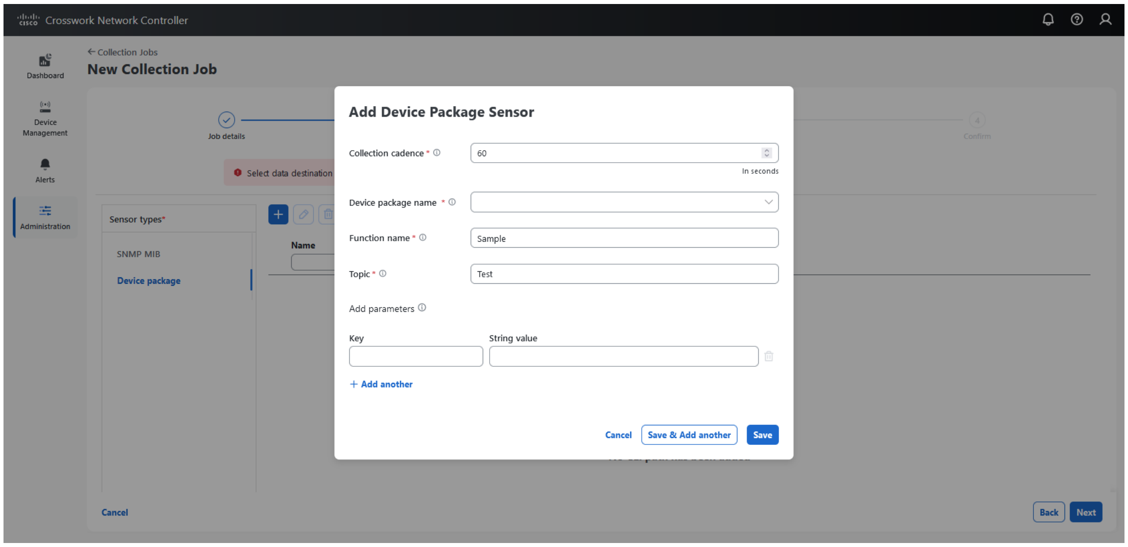
Topic * Sample

- 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 the + button and enter values for the following parameters in the **Add Device Package Sensor** dialog box:

Figure 38: Add Device Package Sensor Dialog Box



Add Device Package Sensor

Collection cadence * 60 (In seconds)

Device package name *

Function name * Sample

Topic * Test

Add parameters

Key

String value

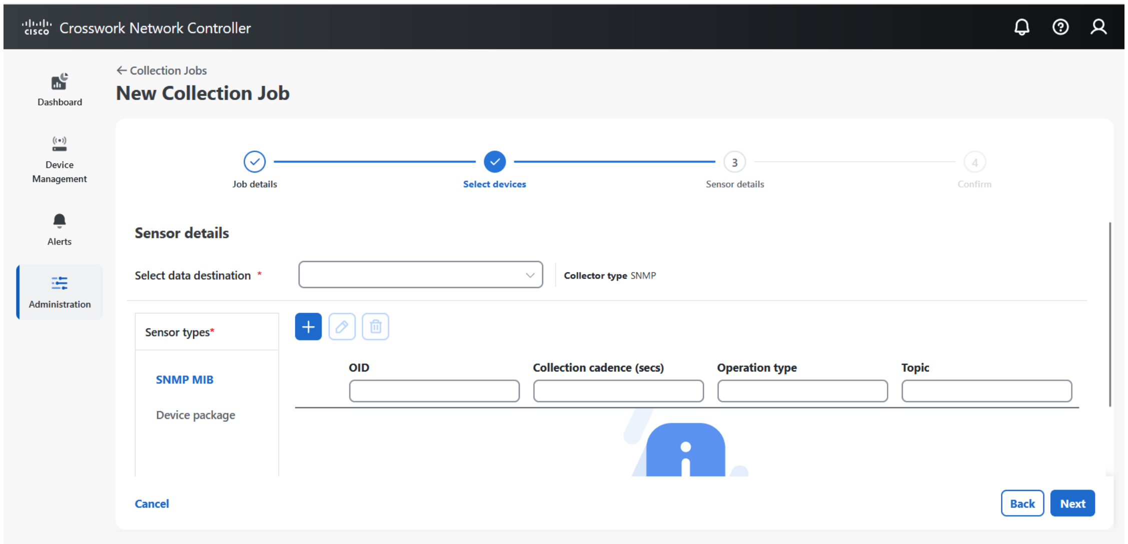
- Collection cadence: Push or poll cadence in seconds.
- Device package name: Custom XDE device package ID used while creating the device package.

- Function name: Function name within a custom XDE device package.
- Topic: Topic associated with the output destination.
- Enter the Key and String value for the parameters.

Click **Save**.

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

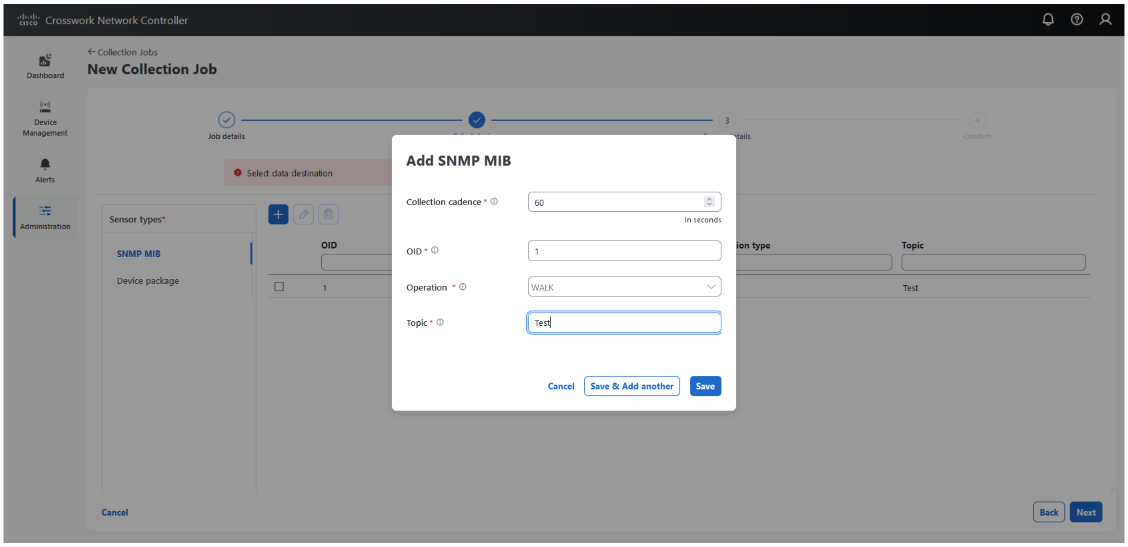
Figure 39: Sensor Details Window for SNMP Path



- Select a data destination from the **Select data destination** drop-down list.
- Select the sensor type from the **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 40: Add SNMP MIB Dialog Box



Add SNMP MIB

Collection cadence *: 60 (In seconds)

OID *: 1

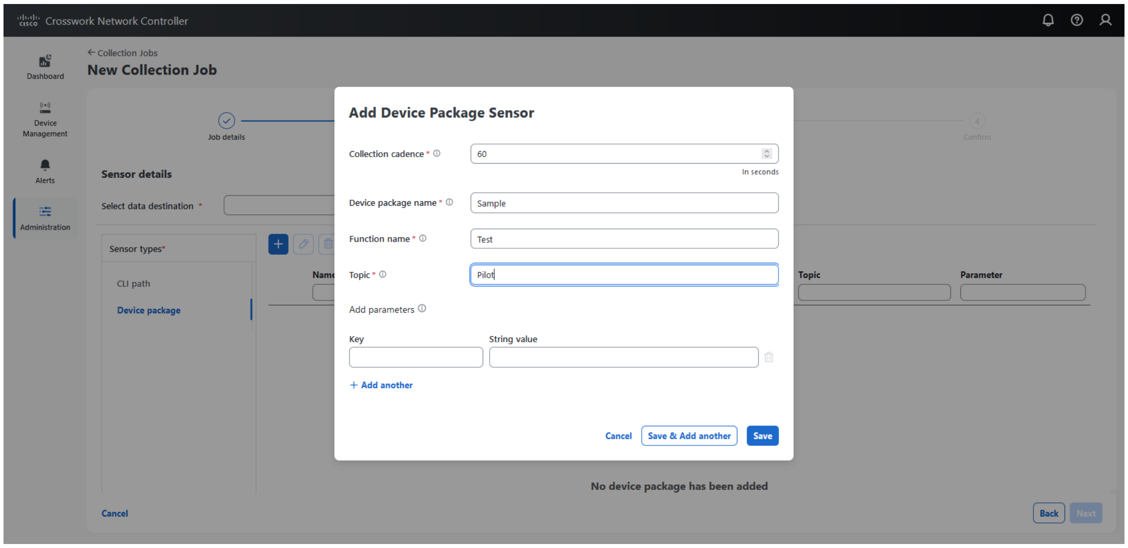
Operation *: WALK

Topic *: Test

- 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 the + button and enter values for the following parameters in the **Add Device Package Sensor** dialog box:

Figure 41: Add Device Package Sensor Dialog Box



Add Device Package Sensor

Collection cadence *: 60 (In seconds)

Device package name *: Sample

Function name *: Test

Topic *: Pilot

Add parameters

Key:

String value:

- Collection cadence: Push or poll cadence in seconds.
- Device package name: Custom device package ID used while creating the device package.

- Function name: Function name within a custom device package.
- Topic: Topic associated with the output destination.
- Enter the 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 that is, 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 is 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 the port is blocked on an external Kafka VM. You can use the following command to check if the 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 Crosswork Network Controller 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, Context ID, and Actions. The Actions drop-down lets you:

- Delete: Removes a collection job.
- Refresh: Refreshes the status of the collection job and the tasks associated with the job.

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 an 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. Crosswork Network Controller 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.

Crosswork Network Controller 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.
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.

Field	Description
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 Errors that occur when the creation or deletion procedure fails are displayed in a separate pop-up screen. 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 causes collection issues. Jobs created by Health Insights should only be deleted by disabling the KPI profile which will remove the collection jobs it deployed. When you delete a collection job, it deletes the associated collection tasks.

Use this procedure to delete external collection jobs from the **Collection Jobs** page. Follow the steps to delete a collection job:

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

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

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

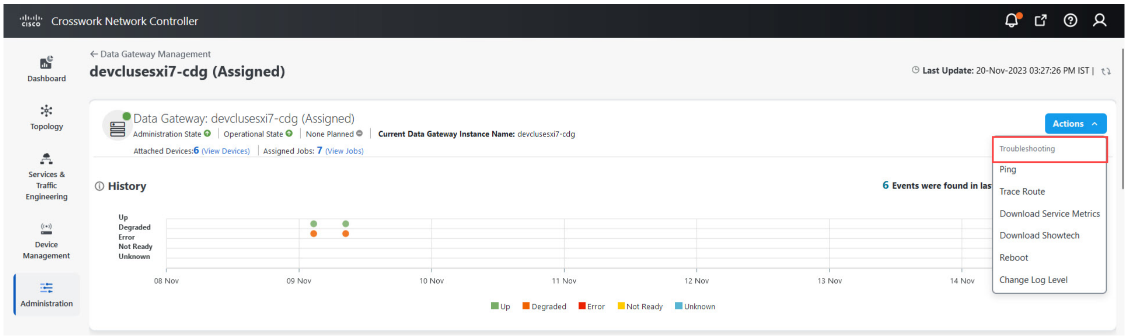
Step 4 In the corresponding row, click ⋯ and select **Delete**. The **Delete Collection Job** window is displayed.

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

Troubleshoot Crosswork Data Gateway

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

Figure 42: Data Gateway - Troubleshooting



Crosswork Network Controller

Data Gateway Management

devclusesxi7-cdg (Assigned)

Last Update: 20-Nov-2023 03:27:26 PM IST

Data Gateway: devclusesxi7-cdg (Assigned)

Administration State | Operational State | None Planned | Current Data Gateway Instance Name: devclusesxi7-cdg

Attached Devices:6 (View Devices) | Assigned Jobs: 7 (View Jobs)

History

6 Events were found in las

For details on troubleshooting options available from the Interactive Console of the data gateway VM, see Troubleshooting Crosswork Data Gateway VM.

Check Connectivity to the Destination

To check connectivity to a destination from a 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 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 data gateway from the Cisco Crosswork UI.

Step 1 Go to **Administration** > **Data Gateway Management** > **Data gateway instances**.

Step 2 Click the 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:

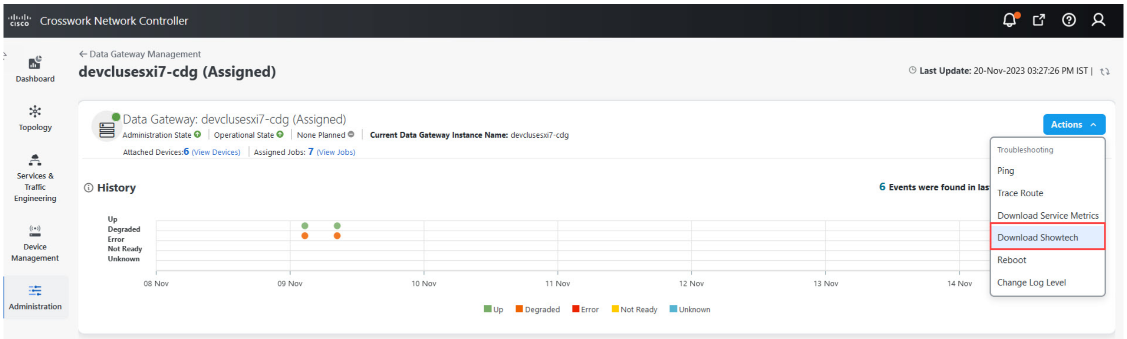
Note Showtech logs cannot be collected from the UI if the data gateway is in an ERROR state. In the DEGRADED state of data gateway, if the OAM-Manager service is running and not degraded, you will be able to collect logs.

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

Step 2 Click the 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**.

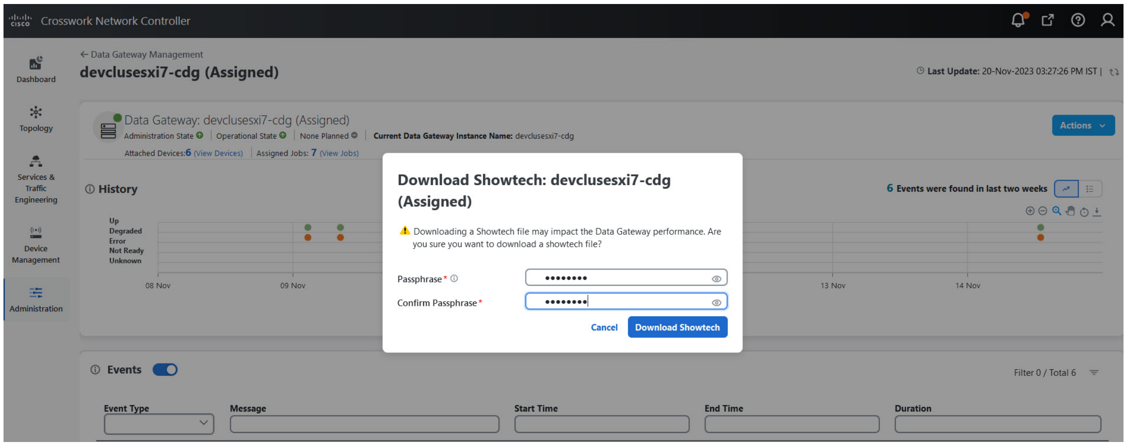
Figure 43: Data Gateway - Download Showtech


Crosswork Network Controller
Dashboard
Topology
Services & Traffic Engineering
Device Management
Administration
← Data Gateway Management
devclusesxi7-cdg (Assigned)
Last Update: 20-Nov-2023 03:27:26 PM IST |
Data Gateway: devclusesxi7-cdg (Assigned)
Administration State | Operational State | None Planned | Current Data Gateway Instance Name: devclusesxi7-cdg
Attached Devices: 6 (View Devices) | Assigned Jobs: 7 (View Jobs)
Actions
History
6 Events were found in las
Up
Degraded
Error
Not Ready
Unknown
08 Nov
09 Nov
10 Nov
11 Nov
12 Nov
13 Nov
14 Nov
Troubleshooting
Ping
Trace Route
Download Service Metrics
Download Showtech
Reboot
Change Log Level
Up
Degraded
Error
Not Ready
Unknown

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 44: Download Showtech Pop-up Window


Crosswork Network Controller
Dashboard
Topology
Services & Traffic Engineering
Device Management
Administration
← Data Gateway Management
devclusesxi7-cdg (Assigned)
Last Update: 20-Nov-2023 03:27:26 PM IST |
Data Gateway: devclusesxi7-cdg (Assigned)
Administration State | Operational State | None Planned | Current Data Gateway Instance Name: devclusesxi7-cdg
Attached Devices: 6 (View Devices) | Assigned Jobs: 7 (View Jobs)
Actions
History
6 Events were found in last two weeks
Up
Degraded
Error
Not Ready
Unknown
08 Nov
09 Nov
13 Nov
14 Nov
Events
Filter 0 / Total 6
Event Type
Message
Start Time
End Time
Duration

Download Showtech: devclusesxi7-cdg (Assigned)

⚠ Downloading a Showtech file may impact the Data Gateway performance. Are you sure you want to download a showtech file?

Passphrase * ••••••••

Confirm Passphrase * ••••••••

Cancel | Download Showtech

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 Data Gateway VM

Follow the steps to reboot a data gateway from the Crossword Network Controller UI:

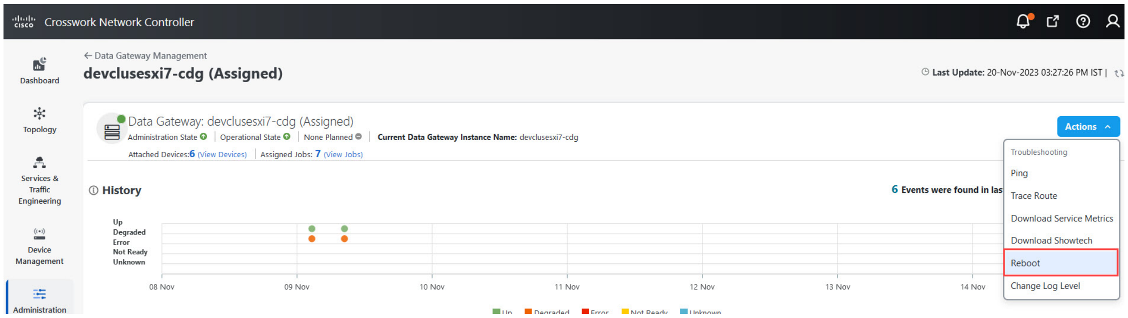
Note Rebooting the data gateway pauses its functionality until it is up again.

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

Step 2 Click the 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 45: Data Gateway - Reboot



devclusesxi7-cdg (Assigned)

Last Update: 20-Nov-2023 03:27:26 PM IST |

Data Gateway: devclusesxi7-cdg (Assigned)

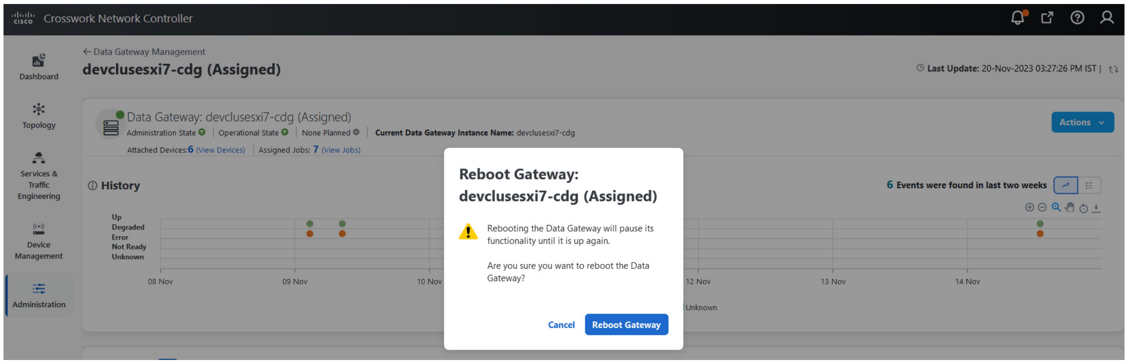
Administration State | Operational State | None Planned | Current Data Gateway Instance Name: devclusesxi7-cdg

Attached Devices:6 (View Devices) | Assigned Jobs: 7 (View Jobs)

6 Events were found in las

Step 4 Click **Reboot Gateway**.

Figure 46: Reboot Gateway Popup Window



devclusesxi7-cdg (Assigned)

Last Update: 20-Nov-2023 03:27:26 PM IST |

Data Gateway: devclusesxi7-cdg (Assigned)

Administration State | Operational State | None Planned | Current Data Gateway Instance Name: devclusesxi7-cdg

Attached Devices:6 (View Devices) | Assigned Jobs: 7 (View Jobs)

6 Events were found in last two weeks

Reboot Gateway: devclusesxi7-cdg (Assigned)

Rebooting the Data Gateway will pause its functionality until it is up again.

Are you sure you want to reboot the Data Gateway?

Once the reboot is complete, check the operational status of the 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 data gateway on which you are making the change.

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

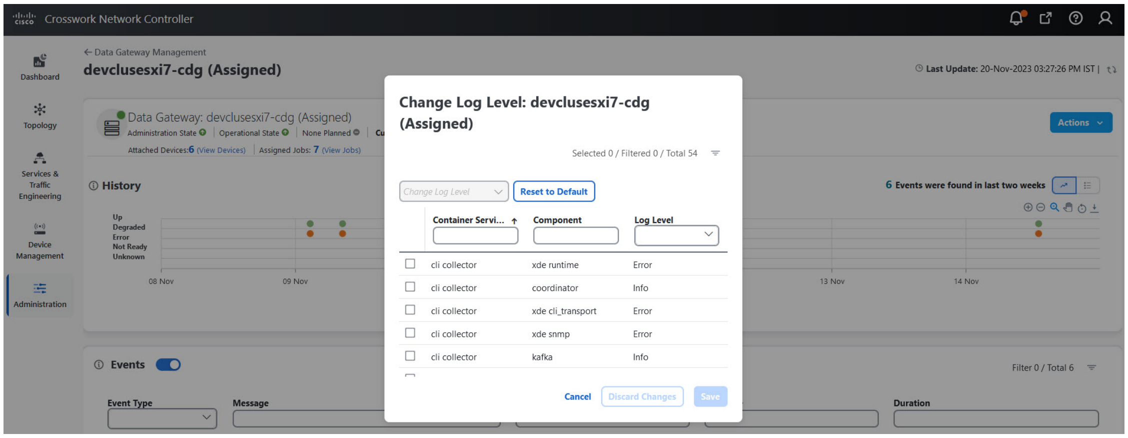
Step 1 Go to **Administration** > **Data Gateway Management** > **Data gateways**.

Step 2 Click the 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 47: Change Log Level Window


Crosswork Network Controller
Dashboard
Topology
Services & Traffic Engineering
Device Management
Administration
← Data Gateway Management
devclusesxi7-cdg (Assigned)
Last Update: 20-Nov-2023 03:27:26 PM IST
Data Gateway: devclusesxi7-cdg (Assigned)
Actions
History
6 Events were found in last two weeks
Events
Filter 0 / Total 6
Event Type
Message
Duration

Change Log Level: devclusesxi7-cdg (Assigned)

Selected 0 / Filtered 0 / Total 54

Change Log Level | Reset to Default

	Container Servi...	Component	Log Level
□	cli collector	xde runtime	Error
□	cli collector	coordinator	Info
□	cli collector	xde cli_transport	Error
□	cli collector	xde snmp	Error
□	cli collector	kafka	Info

Cancel | Discard Changes | Save

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.

Unable to Move Data Gateway from Assigned to Unassigned State

In the **Create Pool** page, under the **Add data gateway instance(s) to pool** pane, data gateways in the Assigned state cannot be moved to the Unassigned state even if they have no devices attached. This indicates that the data gateway has a VIP assigned and cannot be removed from the HA pool.

To remove a data gateway out of the HA pool while it is in the Assigned state, follow these steps:

1. Add an additional data gateway to the ha-pool, only if there isn't already one present as a spare.
2. Perform a manual failover to make the assigned data gateway a spare.
3. Update the HA pool to decrement the spare count and move the spare data gateway out of the pool.

Workaround: If there is an issue with manual failover in **step 2** and the data gateway cannot be converted as spare, delete the HA pool and re-create the pool with a different data gateway. For more information on deleting a gateway, see Delete Crosswork Data Gateway Instance from Crosswork Network Controller.

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, you can review the service status for more information.

To check the service status, go to **Administration** > **Data Gateway Management** > **Data gateways** and click the pool name in the table. The pool details page opens. Navigate to the **Service status** section and review the status details. The section displays a table providing the list of services on the system and the collector responsible for running the job.

If the collector is not listed in the **Service status** section, use the following:

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**.

Step 4 If required, check the status of services in the Service status section.

Data Gateway Collects Data Despite SNMPv3 Engine ID Change

When the SNMPv3 engine ID changes and the device has downtime or reachability issues, the SNMP collector still collects data. Ideally, the data gateway should pause collection during such changes.

The data collection continues even with the **Force Re-Sync USM Engine Details for SNMPV3** option in a disabled state.

To resolve this issue, enable **Force Re-Sync USM Engine Details for SNMPV3** in the Global Parameters window or change the device admin state from DOWN to UP. For more information about enabling the resync option, see Configure Crosswork Data Gateway Global Parameters, on page 44.

The L2VPN Point to Point Service becomes Unresponsive in the Monitoring Initiated State

If the device cannot establish a connection with Data Gateway correctly, the gNMI collection job fails with an error. As a result, the L2VPN Point to Point service cannot monitor the devices, and the status in the Crosswork UI displays as Monitoring initiated.

Workaround: To resume the data collection, detach and reattach the devices with Crosswork Data Gateway. For more information, see:

- Reattach the devices: Attach Devices to a Crosswork Data Gateway, on page 19
- Detach the devices: Manage Crosswork Data Gateway Device Assignments, on page 27

Error Message Pop-up is not Clearly Indicating the IPv6 Address and Port Number

You can check the status summary of devices on the Crosswork Network Controller UI by navigating to **Device Management** > **Network Devices**.

If a device is in the error state, you can see more details by hovering over the information icon next to the state in the **Operational state** column. When dealing with devices that have an IPv6 address, the message displays the address in this format: 2001:420:284:2004:4:112:165:636:22, where the address and port numbers are combined.

In these cases, the first block indicates the address followed by the port number. For example, [2001:420:284:2004:4:112:165:636] is the address, and 22 is the port number. The port number is unavailable if the IP address has only eight segments.

DAD Failure Error During a Failover

During a failover, the primary data gateway (cdg1) switches over to the secondary gateway (cdg2), and cdg2 takes on the southbound IPv6 address of cdg1. When cdg2 is detected, the Crosswok logs an event for cdg2, indicating a Duplicate Address Detection (DAD) failure due to the IP address being a duplicate configuration from dg1. This transient error occurs while the operating system removes the DAD failed flag from the interface. When the operating system clears the DAD failed status from the interface, Crosswork moves the gateway to the **UP** state.

Suppose the DAD failure error persists for more than 2 minutes. In that case, we recommend manually changing the southbound VIP address of the secondary data gateway's HA pool and reinitiating the failover.

Data Gateway Failover Failed

If the failover is not complete due to some issue, reattempt the failover after confirming you have at least one 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 to **NOT_READY**.