Crosswork Data Gateway setup, management, and troubleshooting

This chapter introduces the Crosswork Data Gateway and its core functionalities, guides users through the setup process for data collection, explains how to manage post-setup operations, details the configuration of global settings and data collection jobs, and covers troubleshooting options, outlining common issues, and providing guidance on their diagnosis and resolution.

Crosswork Data Gateways

Crosswork Data Gateway, also referred to as Data Gateway, is a secure, common collection platform for gathering network data from multivendor devices that

- operates as an on-premises application deployed close to network devices
- supports multiple data collection protocols such as SNMP, CLI, gNMI, and Syslog, and
- enables consistent data collection across heterogeneous device environments.

Components of Crosswork Data Gateway

The Data Gateway consists of several core components, each of which plays a crucial role in its deployment, performance, security, and scalability.

The Data Gateway, deployed with Crosswork Infrastructure, is managed by Cisco Crosswork Network Controller and is based on these concepts:

- Crosswork Data Gateway: A deployed Data Gateway instance that you install, which can be associated with the fully qualified domain name, known as FQDN, of a Network Load Balancer, known as NLB, or assigned a virtual IP address when added to a pool. See Cisco Crosswork Installation Requirements in the Installation Guide for Cisco Crosswork Network Controller 4.5 on Amazon EKS for instance requirements.
- Profile: Determines the deployment profile for the Data Gateway:
  - Standard: for use with all Crosswork applications except Crosswork Health Insights and Crosswork Service Health (Automated Assurance)
  - Extended: for Crosswork Health Insights and Crosswork Service Health (Automated Assurance)

Note The **Standard with Extra Resources** profile is a limited-availability feature and must not be used when deploying a Data Gateway in your data center.

- Crosswork Data Gateway pool: A logical group of one or more Data Gateway instances, with optional high availability. If one instance fails, another instance in the pool replaces it to minimize disruption.
- Data destination: Internal or external recipients that receive data collected by the Data Gateway. By default, Cisco Crosswork acts as a data destination, but other external destinations can be defined using the Cisco Crosswork UI or APIs.
- Collection job: A task created to collect data, such as checking device reachability or collecting telemetry data for service and network health. Collection jobs can also be configured for non-Crosswork applications using the Crosswork Network Controller UI or APIs.
- Custom software packages: Device model definitions and files used to extend device coverage and enable data collection from devices.

High availability and pools

A Data Gateway high availability pool is a group of Crosswork Data Gateway instances that

- provides device-specific data collection with minimal disruption
- enables high availability by supporting active and standby roles, and
- automatically assigns workloads to standby instances when a failure is detected.

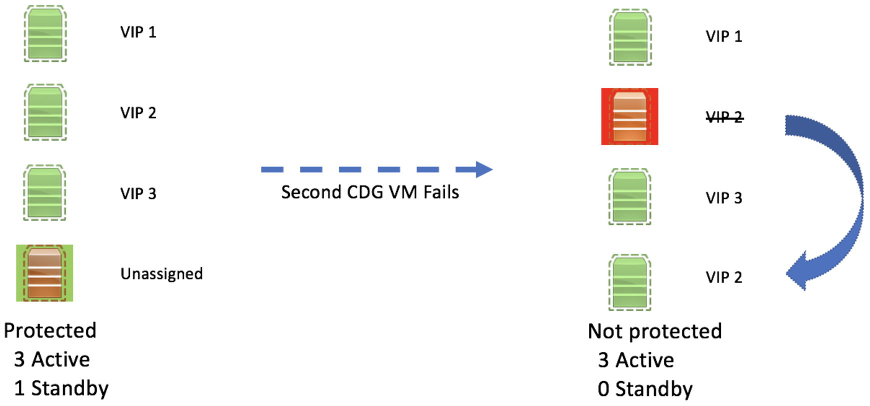
A Data Gateway pool can be in one of several states:

- Protected: All instances are UP, with matched pairs of active and standby
- Not protected: All standby instances are DOWN; none are available to replace an active
- Limited protection: At least one standby instance is UP
- None planned: No standby instances were configured

Understanding Data Gateway failover in an HA environment

CDG1 (active), which has a southbound IP address, becomes unresponsive due to port failures or cable disconnections. The Crosswork Network Controller detects this outage and activates CDG2 (standby) to replace CDG1. At that point, CDG1 and its replacement share the same device-facing IP address. Therefore, you must power off any failed Data Gateway (using VMware) to avoid conflicts. Only power it back on after the issue causing unresponsiveness is resolved and the gateway can rejoin the pool.

Figure 1: Data Gateway high availability



Handling Data Gateway errors and recovery

The Data Gateway manager conducts liveliness checks every 10 seconds; after six missed checks (~60 seconds), a Data Gateway is set to ERROR. If a Data Gateway in a protected pool enters ERROR, devices and jobs are reassigned to a standby instance, ensuring continuity. When a failed instance recovers, it rejoins the pool as standby.

If the Data Gateway identifies interface connectivity issues for northbound communication as part of its 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.

Data Gateway UI structure

This section introduces the user interface elements that help you maximize the capabilities of Data Gateway. It also provides guidance on navigating these elements efficiently.

An overview of the Data Gateway UI structure and its key features and controls offers essential information for navigating and managing Data Gateway VMs effectively.

- The Data Gateway UI equips administrators with comprehensive tools to monitor, filter, and manage pools for streamlined network operations. For information on navigating through the Data Gateway UI, see Access the Data Gateway UI, on page 4.
- Familiarity with the Crosswork Data Gateway UI components allows you to navigate the Crosswork UI easily and efficiently. For more information, see Data Gateway UI components, on page 5.

Access the Data Gateway UI

The Data Gateway user interface provides administrators with tools to monitor, filter, and manage pools efficiently.

Before you begin

Ensure that you are familiar with the Crosswork Network Controller user interface.

Use these steps to access and use the Data Gateway user interface.

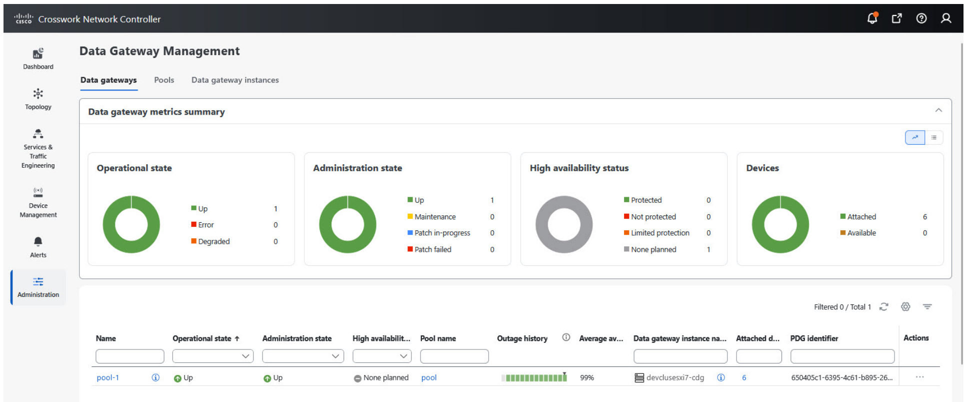
Procedure

Step 1 Log in to Cisco Crosswork Network Controller.

Step 2 Go to **Administration** > **Data Gateway Management**.

Step 3 Use the donut chart legends to filter the table by administration state.

Figure 2: Data Gateway management



Operational state

🟩 Up	1
🟥 Error	0
🟧 Degraded	0

Administration state

🟩 Up	1
🟨 Maintenance	0
🟦 Patch in-progress	0
🟥 Patch failed	0

High availability status

🟩 Protected	0
🟥 Not protected	0
🟧 Limited protection	0
⬜ None planned	1

Devices

🟩 Attached	6
🟧 Available	0

Filtered 0 / Total 1

Name	Operational state ↑	Administration state	High availabilit...	Pool name	Outage history	Average av...	Data gateway instance na...	Attached d...	PDG identifier	Actions
pool-1	Up	Up	None planned	pool		99%	devclusesxi7-cdg	6	650405c1-6395-4c61-b895-26...	···

To view pools with the administration state **Up**, click the **Up** icon next to the chart.

The table displays only pools with the selected state.

Step 4 Show or hide columns in the pools table using the **Settings** menu.

Step 5 Select or clear multiple items using the table's selection controls.

You can now monitor and manage pools using the Data Gateway interface's filtering and selection features.

Data Gateway UI components

Provide an overview of the Data Gateway user interface components, including descriptions of the various tabs and table columns available on the Data Gateway Management page, to help users understand and navigate the Data Gateway UI.

The **Data Gateway Management** page has three tabs.

- **Data gateways**: Displays details of the virtual Data Gateway instances 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 the virtual Data Gateway instances.

This table explains the various columns in the **Data Gateway Managements** page.

Table 1: Data Gateway user interface components

Column	Description
Operational State	Operational state of the Data Gateway instance. A Data Gateway has these operational states: • Degraded: The Data Gateway is reachable but one or more of its components are in a state other than OK. • Up: The Data Gateway 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 these: • Up: The instance is administratively up. • Maintenance: Operations between Cisco Crosswork and Data Gateway are suspended to perform upgrades or other maintenance activities (for example, uploading certificates). • Patch in progress: The process of installing or applying a patch on the Data Gateway is currently ongoing. • Patch failed: The process of installing or applying a patch on the Data Gateway failed. An info icon appears only when the administration state is **Patch failed**. Click ⓘ to view detailed failure information.

Column	Description
High availability status	High availability status of a Data Gateway could be either: • Protected: All instances are in the UP state, and the number of standby instances in the pool matches the number of active instances. • Not protected: All standby instances are DOWN. • Limited protection: At least one standby instance in the pool is in the UP state. • None planned: No standby instances were added to the pool during pool creation.
Devices	Number of devices that are attached to the Data Gateway pool.
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 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 enabled. For information on the geo redundancy capabilities, see the *Enable Geo Redundancy* section in the *Cisco Crosswork Network Controller 7.2 Installation Guide*.

Column	Description
Data gateway instance role	Indicates the current role of the Data Gateway instance. The role could be any of these: • 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 is used during failover process in an active site. • Spare (Standby): The Data Gateway instance acts as a spare instance for failover procedures in a standby site.
Outage history	Outage history of the Data Gateway instance over a period of 14 days. State aggregation for a day follows this order of precedence: Error, Degraded, Up, Unknown, and Not Ready. For example, if the Data Gateway instance went Unknown to Degraded to Up, the 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 was in Degraded state at any time during the day, the tile is orange. If the Data Gateway was not in Error or Degraded state and was only Up during the day, 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 the 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 timestamp, so the duration of the last event is between its start time and the current timestamp.

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, type, role, UUID, OS version • Description • CPU • Memory • Number of NICs • Interface roles, MAC, IPv4 and IPv6 address 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 Data Gateway, on page 23. • Detach devices. For more information, see Detach devices from Data Gateway, on page 25. • Move devices. For more information, see Move devices to a different Data Gateway, on page 24. • Initiate a failover. For more information, see Perform a manual failover, on page 20.

Setting up Data Gateways for data collection

Before setting up the Data Gateways, you must understand how Crosswork is set up. For more information, see *Setup workflow* section in the *Get Up and Running (Post-Installation)* chapter.

Summary

This process explains how to configure Crosswork Data Gateway for collecting and transmitting data to Cisco Crosswork and other applications. It describes the setup tasks required for basic operation and outlines optional configurations to extend data collection capabilities. Before beginning, install Crosswork Data Gateway as described in *Cisco Crosswork Network Controller 7.2 Installation Guide*.

Workflow

These are the stages of setting up Crosswork Data Gateway for data collection.

1. Initial Data Gateway configuration

    - Create the Data Gateway pools. See Create a Data Gateway pool, on page 11.
    - (Optional) Create the Data Gateway pools in geo-redundancy sites. See Create a pool in the geo redundancy-enabled sites, on page 15.
    - Attach devices to the Data Gateway. See Attach devices to Data Gateway, on page 23.
    - Verify that the default collection jobs are created and are running successfully. See Monitor the collection jobs, on page 65.

2. Extending Data Gateway capabilities (Optional).

    This stage describes optional configurations that extend the Data Gateway's capabilities.

Table 2: Setting up the Data Gateway

When the user wants to...	Then refer to the steps in...
Extend device coverage to collect data from currently unsupported devices or third-party devices.	Device package management, on page 52
Forward data to external data destinations.	External data destinations, on page 39
Create custom collection jobs that function independently from those built by Cisco Crosswork.	Create a collection job from Crosswork UI , on page 59

Result

When these stages are complete, Crosswork Data Gateway collects and transmits data to Cisco Crosswork and other configured applications. You can configure advanced features to further extend its capabilities.

Data Gateway pool operations

Crosswork Data Gateway pools are essential for ensuring scalable, resilient, and efficient network data collection in enterprise environments. The primary use case is to group multiple Crosswork Data Gateway instances into logical pools, which enables high availability, automatic failover, and balanced data ingestion for large-scale or mission-critical operations. You can use these operations to interact with pools:

- Create a Data Gateway pool, on page 11
- Create a pool in the geo redundancy-enabled sites, on page 15
- Assign Data Gateways to geo redundancy-enabled sites, on page 18
- Edit or delete a Data Gateway pool, on page 19

High availability and pools

A Data Gateway high availability pool is a group of Crosswork Data Gateway instances that

- provides device-specific data collection with minimal disruption
- enables high availability by supporting active and standby roles, and
- automatically assigns workloads to standby instances when a failure is detected.

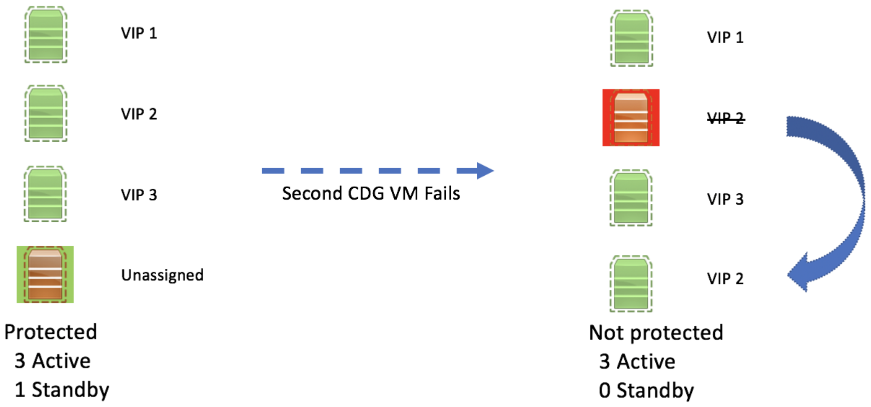
A Data Gateway pool can be in one of several states:

- Protected: All instances are UP, with matched pairs of active and standby
- Not protected: All standby instances are DOWN; none are available to replace an active
- Limited protection: At least one standby instance is UP
- None planned: No standby instances were configured

Understanding Data Gateway failover in an HA environment

CDG1 (active), which has a southbound IP address, becomes unresponsive due to port failures or cable disconnections. The Crosswork Network Controller detects this outage and activates CDG2 (standby) to replace CDG1. At that point, CDG1 and its replacement share the same device-facing IP address. Therefore, you must power off any failed Data Gateway (using VMware) to avoid conflicts. Only power it back on after the issue causing unresponsiveness is resolved and the gateway can rejoin the pool.

Figure 3: Data Gateway high availability



Handling Data Gateway errors and recovery

The Data Gateway manager conducts liveliness checks every 10 seconds; after six missed checks (~60 seconds), a Data Gateway is set to ERROR. If a Data Gateway in a protected pool enters ERROR, devices and jobs are reassigned to a standby instance, ensuring continuity. When a failed instance recovers, it rejoins the pool as standby.

If the Data Gateway identifies interface connectivity issues for northbound communication as part of its 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

Use this procedure to create a Data Gateway pool, which groups Data Gateway instances for data collection and enables their configuration for various network environments.

A Data Gateway pool is a group of Data Gateway instances configured for data collection in different network environments. This procedure guides users through creating a pool, choosing its type, entering configuration parameters, and assigning instances, with references to prerequisites and parameter details as needed.

Before you begin

Carefully review the prerequisites and guidelines before creating a Data Gateway pool. For more information, see Requirements to create a Data Gateway pool, on page 13.

Complete these steps to create a Data Gateway pool.

Procedure

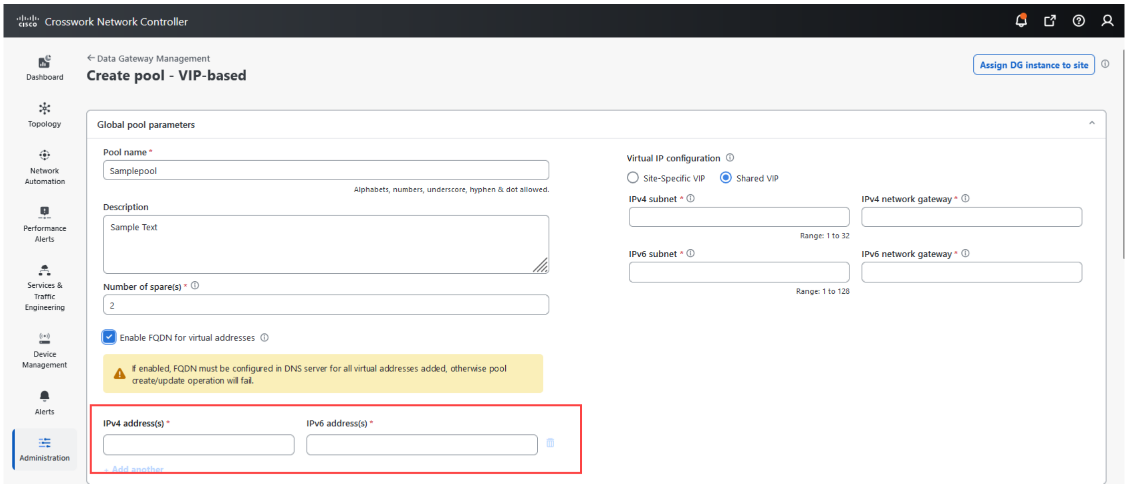
Step 1 Navigate to the **Administration** > **Data Gateway Management** > **Pools** tab.

Step 2 Click + and select one of the options:

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

Step 3 In the **Pool parameters** pane, enter the required pool parameters. For a list of parameters, see Pool parameters, on page 14.

Figure 4: VIP-based pool for single stack deployment


Crosswork Network Controller
Dashboard
Topology
Network Automation
Performance Alerts
Services & Traffic Engineering
Device Management
Alerts
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 addresses

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

IPv4 address(s) *

IPv6 address(s) *

Virtual IP configuration

○ Site-Specific VIP ● Shared VIP

IPv4 subnet * Range: 1 to 32

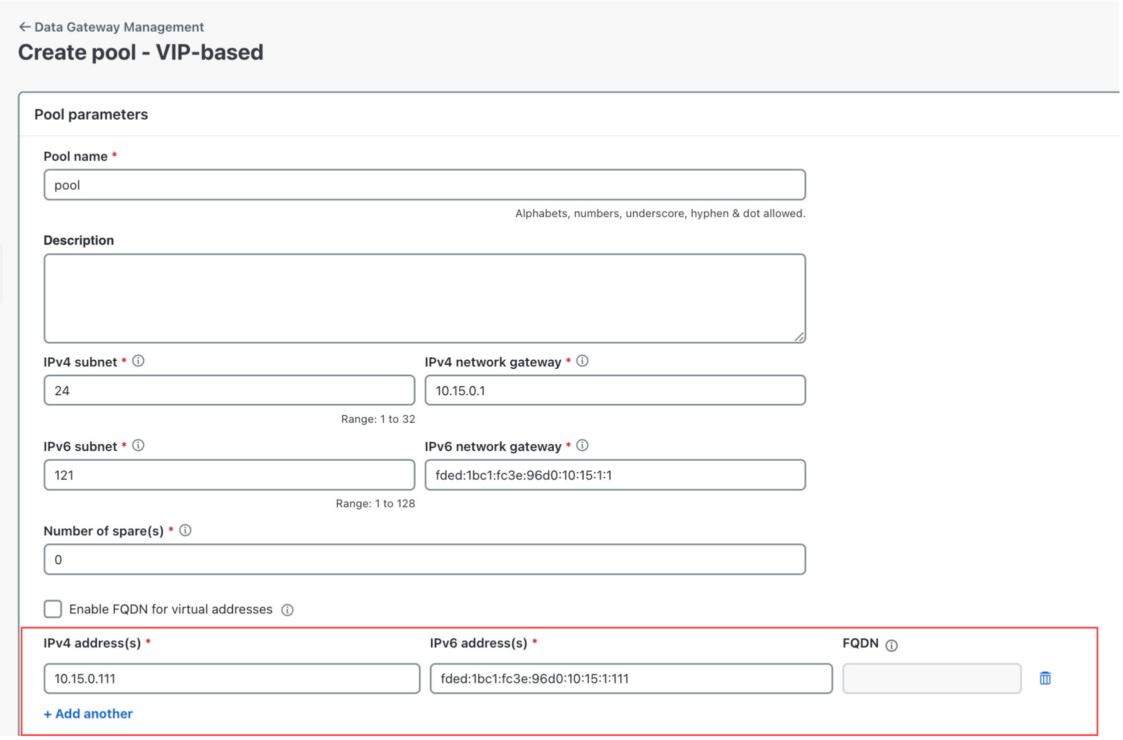
IPv4 network gateway *

IPv6 subnet * Range: 1 to 128

IPv6 network gateway *

Step 4 (Optional) Specify both the VIP IPv4 and IPv6 addresses when creating a pool for a dual-stack deployment.

Figure 5: VIP-based pool for dual-stack deployment



← Data Gateway Management

Create pool - VIP-based

Pool parameters

Pool name *: pool

Alphabets, numbers, underscore, hyphen & dot allowed.

Description:

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

IPv4 network gateway *: 10.15.0.1

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

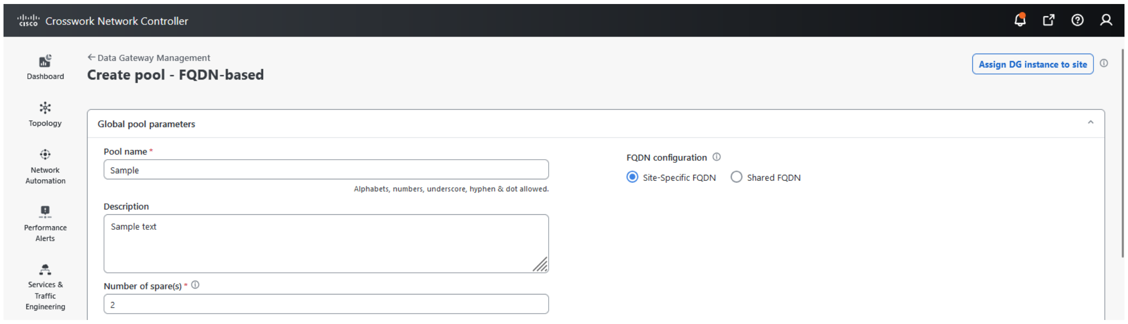
IPv6 network gateway *: fded:1bc1:fc3e:96d0:10:15:1:1

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 6: FQDN-based pool



Crosswork Network Controller
Dashboard
Topology
Network Automation
Performance Alerts
Services & Traffic Engineering
Assign DG instance to site

← Data Gateway Management

Create pool - FQDN-based

Global pool parameters

Pool name *: Sample

Alphabets, numbers, underscore, hyphen & dot allowed.

Description: Sample text

Number of spare(s) *: 2

FQDN configuration: ● Site-Specific FQDN ○ Shared FQDN

Step 5 Add the required Data Gateway instances. Based on your selection, IPv4, IPv6, both, or FQDN, enter a virtual IP address or FQDN for each active Data Gateway instance.

Step 6 In the **Assign data gateway instance(s)** pane, select the Data Gateway instances from **Unassigned data gateway instance(s)**. Click the right arrow to assign the instances to **Assigned data gateway instance(s)**.

Step 7 Click **Create**.

What to do next

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

Requirements to create a Data Gateway pool

Best practice for Data Gateway pool creation

Before you create a Data Gateway pool, adhere to these requirements.

- Install at least one Data Gateway instance for basic operation, or two for high availability.
- Determine the number of Data Gateway instances based on your network needs. If you need assistance, contact the Cisco Customer Experience team.
- Register at least one Data Gateway with Crosswork Network Controller. The operational state of the Data Gateway should be NOT_READY.
- To achieve high availability, deploy multiple Data Gateway instances.
- Distribute Data Gateway instances in each pool to minimize risks from Crosswork or site failure.
- Gather the required network information: one virtual IP for each active Data Gateway, the subnet mask, and Data Gateway details.
- For a 3-NIC deployment, provide the Data Gateway address for network device access.
- For 2-NIC deployment, use an additional IP on the Data Network as the virtual IP. For 3-NIC deployment, use the Southbound Network IP as the virtual IP.

Geo redundancy and syslog requirements

The geo redundancy options are available only when the geo redundancy feature is configrued. For information about the geo redundancy capabilities, see the *Enable Geo Redundancy* section in the *Cisco Crosswork Network Controller 7.2 Installation Guide*.

- Enable secure syslog communication using syslog certificates that contain the hostname or FQDN instead of the virtual IP. If using FQDNs for virtual IPs, configure them in your DNS server before pool creation.
- 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.

FQDN and DNS requirements

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.

Pool setup configuration options

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

- Pool types.
    - 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 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.

- VIP configuration options.
  - 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 Gateway instances 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 Gateway instances 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 that is 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 Crosswork is deployed on a dual-stack, make sure that the Data Gateway instances 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.
- In AWS EC2, a Crosswork Data Gateway pool spanning multiple Availability Zones (AZs) supports only a 1:1 configuration. Each pool includes one active instance and one standby instance. This setup consists of one active Data Gateway and one standby Data Gateway, meaning that each pool can only include one active instance and one standby instance.
- On-premises setups may support M:N configurations, where M is the number of active instances and N is the number of standby instances. In contrast, AWS EC2 supports only the 1:1 redundancy model.

Pool parameters

This section describes the pool parameters required when creating a Data Gateway pool.

Table 3: Pool parameters and descriptions

Parameters	Description
Pool name	Unique name that describes the network
Description	Description of the pool.
IPv4 subnet	IPv4 subnet mask for each Data Gateway; use a value from 1 to 32.
IPv4 network gateway	IPv4 network gateway address to communicate with devices.

Parameters	Description
IPv6 subnet	Subnet mask for each Data Gateway. The IPv6 subnet mask value can be from 1 to 128.
IPv6 network gateway	IPv6 network gateway address to communicate with devices.
Number of spares	Number of Data Gateway instances that operate as standby; if an active Data Gateway is unavailable, a spare assumes the active role
Enable FQDN for virtual IP addresses	Hostname or FQDN for each virtual IP address of the Data Gateway in the syslog certificate.
IPv4 address	IPv4 address of the Data Gateway VMs.
IPv6 address	IPv6 address of the Data Gateway VMs not assigned to any other VM.
FQDN	The FQDN address is not configurable and is fetched from DNS after a successful pool creation or edit operation.

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

Carefully review the prerequisites and guidelines before creating a Data Gateway pool. For more information, see Requirements to create a Data Gateway pool, on page 13.

Procedure

Step 1 Navigate to the **Administration** > **Data Gateway Management** > **Pools** tab.

Step 2 Click + and select one of the options:

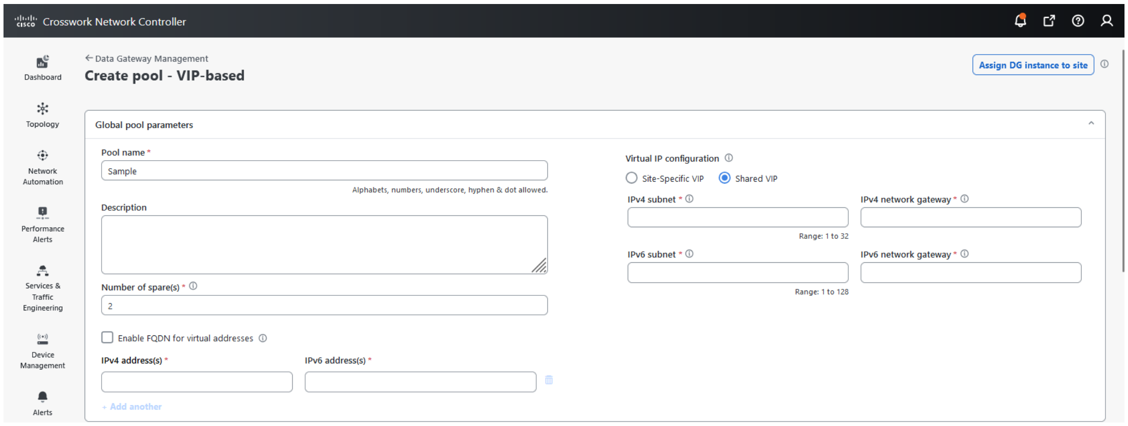
- **VIP-based**
- **FQDN-based**

To view information about the pool types, click **Types of pools** in the top-right corner. The **Create pool** page appears.

Step 3 In the **Pool parameters** pane, enter the required pool parameters. For a list of parameters, see Pool parameters, on page 14.

Step 4 Add the required Data Gateway instances. Based on your selection, IPv4, IPv6, both, or FQDN, enter a virtual IP address or FQDN for each active Data Gateway instance.

Figure 7: VIP-based pool



← Data Gateway Management

Create pool - VIP-based

Global pool parameters

Pool name * Sample

Alphabets, numbers, underscore, hyphen & dot allowed.

Description

Number of spare(s) * 2

☐ Enable FQDN for virtual addresses

IPv4 address(s) *

IPv6 address(s) *

Virtual IP configuration

○ Site-Specific VIP ● Shared VIP

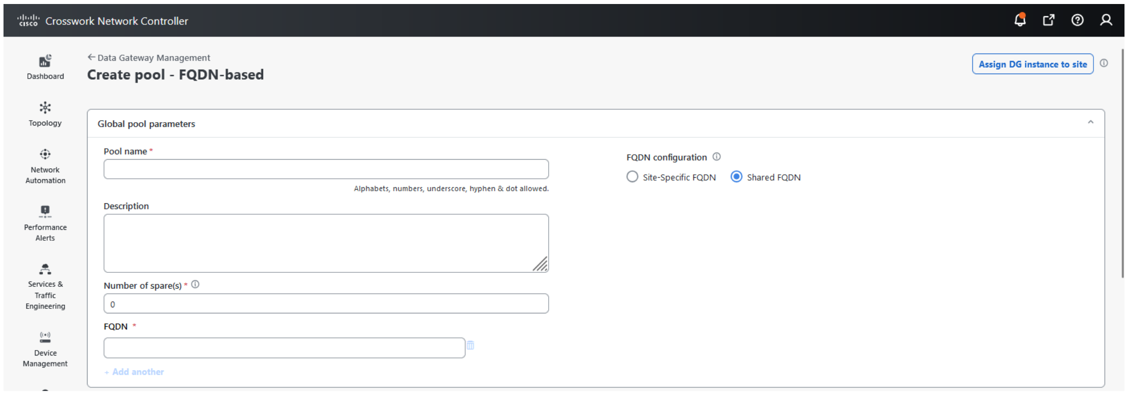
IPv4 subnet * Range: 1 to 32

IPv4 network gateway *

IPv6 subnet * Range: 1 to 128

IPv6 network gateway *

Figure 8: FQDN-based pool


Crosswork Network Controller
Dashboard
Topology
Network Automation
Performance Alerts
Services & Traffic Engineering
Device Management
Assign DG instance to site
+ Add another

← Data Gateway Management

Create pool - FQDN-based

Global pool parameters

Pool name *

Alphabets, numbers, underscore, hyphen & dot allowed.

Description

Number of spare(s) * 0

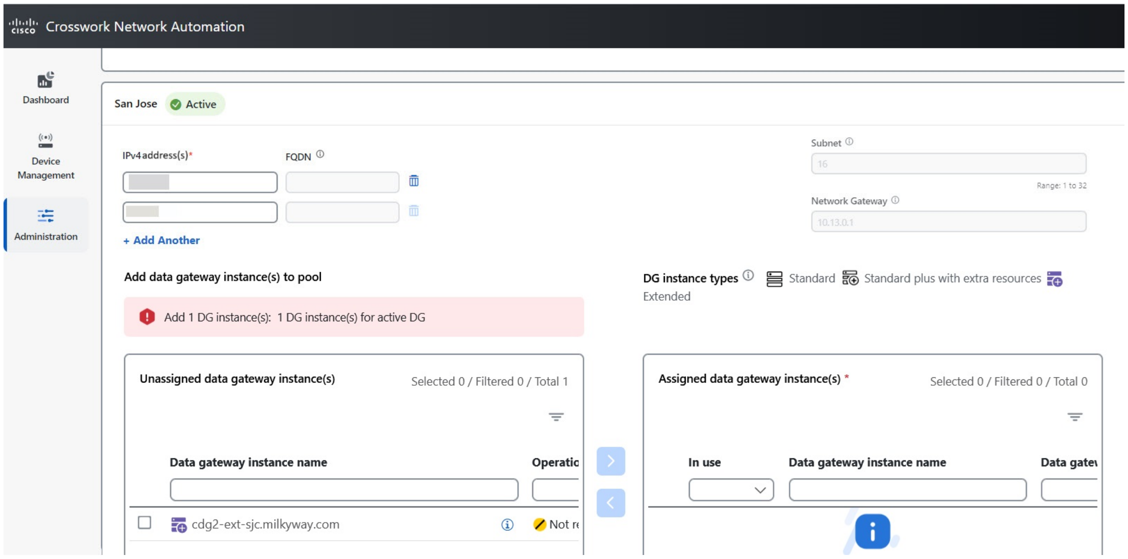
FQDN *

FQDN configuration

○ Site-Specific FQDN ● Shared FQDN

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)**.

Figure 9: Active pane for single stack



San Jose Active

IPv4address(s)* [redacted] [redacted]

FQDN

Subnet 16 Range: 1 to 32

Network Gateway 10.13.0.1

+ Add Another

Add data gateway instance(s) to pool

Add 1 DG instance(s): 1 DG instance(s) for active DG

DG instance types Standard Standard plus with extra resources Extended

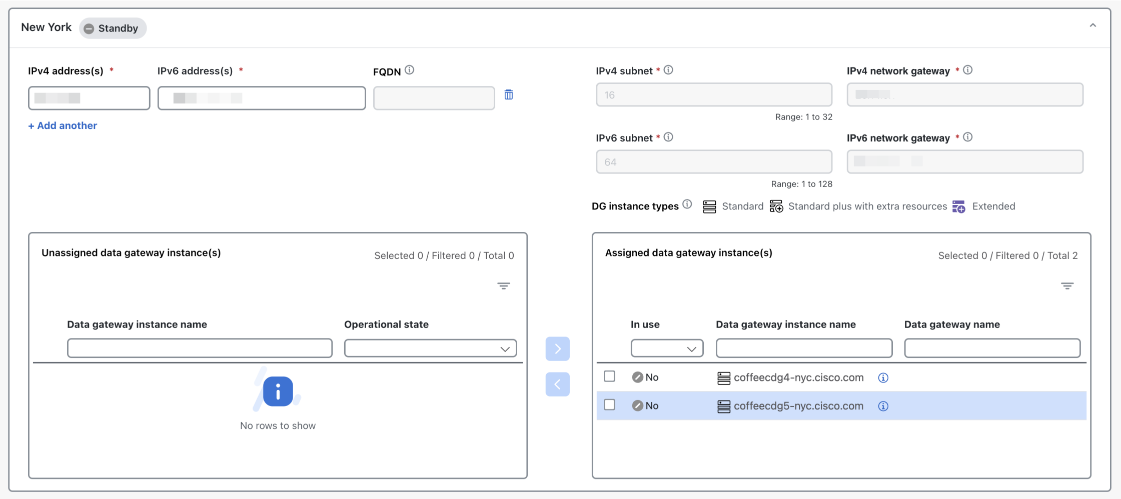
Unassigned data gateway instance(s) Selected 0 / Filtered 0 / Total 1

Data gateway instance name	Operatic
□ cdg2-ext-sjc.milkyway.com	Not r

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

In use	Data gateway instance name	Data gatev

Figure 10: Active pane for dual stack



New York Standby

IPv4 address(s) * [redacted]

IPv6 address(s) * [redacted]

FQDN

+ Add another

IPv4 subnet * 16 Range: 1 to 32

IPv4 network gateway * [redacted]

IPv6 subnet * 64 Range: 1 to 128

IPv6 network gateway * [redacted]

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 6 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**.

Step 7 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 saved your changes, 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 maintain uninterrupted data collection by reassigning a Data Gateway from a standby site to an active geo redundancy-enabled site.

Perform this task to fail over the Data Gateway responsibilities due to site maintenance, upgrades, or unexpected outages to ensure continuous data collection and network operations. By reassigning the Data Gateway, you can continue to maintain data flow continuity. without disruption. This leverages the geo redundant architecture for high availability.

Before you begin

The prerequisites for reassigning a Data Gateway from standby to active site in a Crosswork environment include:

- Confirm that the site has the geo redundancy feature enabled, as Data Gateway instances can only be assigned in such environments. For enabling geo redundancy, see the *Enable Geo Redundancy* section in the *Cisco Crosswork Network Controller 7.2 Installation Guide*.
- Ensure that the Data Gateways are currently unassigned, providing the option to assign them to either the active or standby site.

  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 part of a pool, verify that assignment will be performed during a Crosswork migration process using the edit pool option. During migration, a notification will appear on the **Data Gateway Management** page indicating the ongoing process.
- Validate that the network and resource requirements are met, including sufficient VM resources, bandwidth, and network configurations consistent with the deployment guidelines outlined in the Cisco documentation.

Procedure

Step 1 Navigate to **Administration** > **Data Gateway Management** and choose 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 unassigned Data Gateway instance to be reassigned.

Step 4 Choose the target site from the Select site drop-down list.

Step 5 Click **Assign**.

The selected Data Gateway instance is assigned to the chosen site. The site name is updated in the management interface.

What to do next

Confirm data collection continuity and verify that the Data Gateway is operational at the new site. Monitor for any status alerts after the assignment.

Edit or delete a Data Gateway pool

Before you begin

Prerequisites before editing or deleting a Data Gateway pool:

- Ensure that no devices are currently attached to the virtual Data Gateways or to any pools, as deletion is not allowed while devices remain attached.
- All devices mapped to a Data Gateway instance must be unmapped before you can remove that instance from the pool. Removing the instance allows the system to select a standby instance from the pool as a replacement during a failover operation.
- Prior to deleting a Data Gateway pool, detach all devices from the Data Gateway or migrate them to another Data Gateway instance. For details on manual failover procedures, see Perform a manual failover, on page 20.

Use these steps to edit or delete a Data Gateway pool.

Procedure

Step 1 Navigate to **Administration** > **Data Gateway Management** and choose the **Pools** tab.

Step 2 Edit high availability (HA) pool:

a) Select a pool you want to edit from the list of pools displayed on this page.

b) To open the **Edit high availability (HA) pool** page, click ✎.

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.

c) You can modify the resource parameters that change depending on the pool type in the **Pool parameters** pane:

- Add a virtual IP address or FQDN for each active Data Gateway. For dual-stack deployments, provide both IPv4 and IPv6 addresses.

  Note
  FQDN is not applicable to VIP-based pools because it is fetched from DNS after a successful pool creation or edit operation.

- Change the number of standby Data Gateway instances.
- Add or remove Data Gateway instances from the pool.
- Enable or disable FQDN for the pool.

d) In the **Active** and **Standby** site parameters pane, modify the IP or FQDN addresses of the Data Gateway VM.

The Active and Standby panes are visible only when geo redundancy is enabled. For details about geo redundancy, see the *Enable Geo Redundancy* section in the *Cisco Crosswork Network Controller 7.2 Installation Guide*.

e) Click **Save**.

Step 3 Delete a Data Gateway pool:

a) Select the pool that you want to delete and click 🗑 .

b) To delete a pool, select it and click **Delete** in the **Delete high availability (HA) pool** window.

Perform a manual failover

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

Before you begin

Before initiating a failover in a Data Gateway pool, ensure that you are aware of the considerations:

- 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 simultaneously.
- 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 maintenance mode cannot be used as a spare for future failover procedures until its administration state is UP.
- Ensure that you have the READ and WRITE permissions for the Data Gateway Manager APIs, Platform APIs, and Inventory APIs in Global API permissions. Without them, the corresponding actions will not be available in the Crosswork UI. For information about the permissions, see *Global API Permissions*.

  Alternatively, you can assign the Provisioning permission in Task permissions, and enable both the Data Gateway Manager APIs and Platform APIs in Global API permissions. This action automatically enables the Inventory APIs with READ and WRITE access. These permissions are required to perform device operations such as attach, detach, add, move, and initiate failover. For information about assigning task permissions, see *Assign Task permissions*.

Use these steps to initiate a manual failover of the Data Gateway instance.

Procedure

Step 1 Navigate to the **Administration> Data Gateway Management > Data gateways** tab.

Step 2 Select the Data Gateway you want to fail over.

Step 3 Choose **Initiate failover** from **Actions**.

Step 4 (Optional) If prompted, select to move the Data Gateway to maintenance mode after failover completes.

Step 5 Confirm and continue.

Condense the explanation to main outcomes and highlight follow-up if the action fails.

During failover, the secondary Data Gateway takes over the primary's southbound IPv6 address. Crosswork may log a temporary Duplicate Address Detection (DAD) failure until the operating system clears the DAD flag, after which the Data Gateway shifts to the UP state. If the DAD status is not cleared, investigate IPv6 address conflicts and opertaing system-level DAD handling on the secondary Data Gateway. If the failover is unsuccessful due to an error, see Handle DAD error in Data Gateway failover process, on page 111.

Device assignments and Data Gateway instance management

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

- Administration states of Data Gateways, on page 21
- Attach devices to Data Gateway, on page 23
- Move devices to a different Data Gateway, on page 24
- Detach devices from Data Gateway, on page 25
- Delete the Data Gateway instance from Crosswork Network Controller, on page 26

Administration states of Data Gateways

An administration state is an operational mode that

- controls the availability and maintenance status of Data Gateway
- determines how upgrades and certificate updates are performed, and
- affects communication between Crosswork and the Data Gateway.

The administration states are Up, Maintenance, Patch in-progress, and Patch failed.

Impact of maintenance mode on communication and upgrades

During maintenance, administrators can suspend communication between Data Gateway and Crosswork to perform upgrades. In maintenance mode, certificate updates and other modifications are allowed. Communication interruptions during maintenance temporarily pause job collection, which resumes when the connection is restored.

Note A Data Gateway in the Assigned state cannot directly enter maintenance mode without first executing a manual failover or removing it from the pool.

If an administrator needs to change certificates, they place the Data Gateway in maintenance mode, perform the update, and set the state back to Up. Crosswork Network Controller resumes operations automatically once the Data Gateway is up.

Related Topics

Data Gateway UI components, on page 5

Change the administration state of a Data Gateway

Change a Data Gateway's operational state, for example, to Maintenance mode during upgrades or maintenance.

When performing upgrades or maintenance, it may be necessary to temporarily suspend communication between Crosswork and a Data Gateway by setting the gateway to Maintenance mode. This enables administrators to update configurations or certificates as needed.

Use these steps to change the administration state of a Data Gateway.

Before you begin

Before switching to maintenance mode, ensure that the Data Gateway's role status meets the required conditions.

- Verify that you have READ and WRITE permissions for both Data Gateway Manager APIs and Platform APIs in Global API permissions. Without these, you cannot change administration state via the Crosswork UI. For more information, see *Global API Permissions*.
- Ensure the Data Gateway's role status meets all specified conditions before you change its state.
  - The Data Gateway may have a "Spare" role after failover or may be "Assigned" if it is the only node in a pool.
  - The Data Gateway's role status must comply with these conditions before changing state.

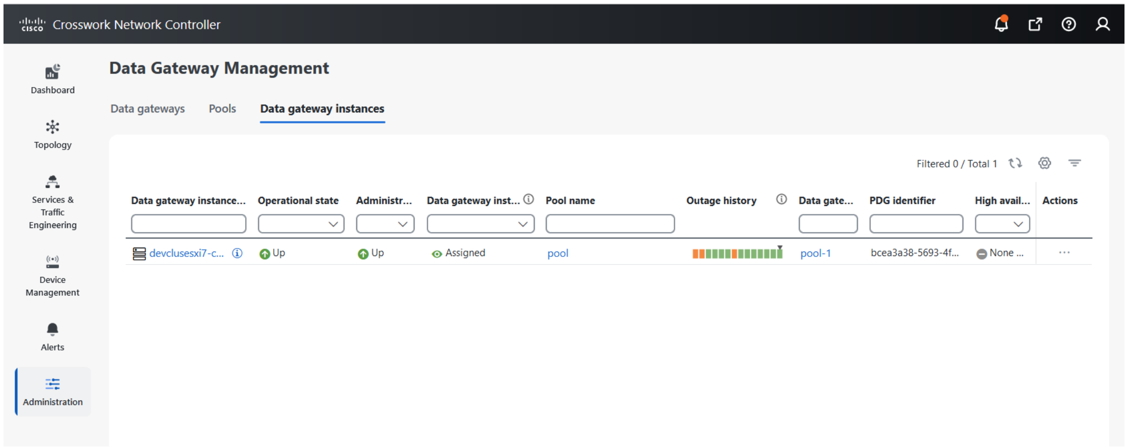
Procedure

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

Click the Data Gateway or pool name in the table to view its operations and health summary; this action opens the details page. To see enrollment details, including interface role information, click the info icon next to the Data Gateway instance name.

Step 2 For the Data Gateway you want to update, click the edit icon under the **Actions** column.

Figure 11: Data gateway instances



Data Gateway Management

Data gateways | Pools | Data gateway instances

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 desired administration state such as "Active" or "Maintenance" for the Data Gateway.

The Data Gateway's administration state is updated, and it is placed into the selected state (for example, Maintenance mode for administrative operations).

What to do next

After maintenance, return the Data Gateway to Active state as needed for normal operation.

Attach devices to Data Gateway

Attach network devices to Crosswork Data Gateway to enable secure, centralized data collection across protocols.

Use this procedure when you need to add new devices for data collection to an existing Crosswork Data Gateway instance.

Before you begin

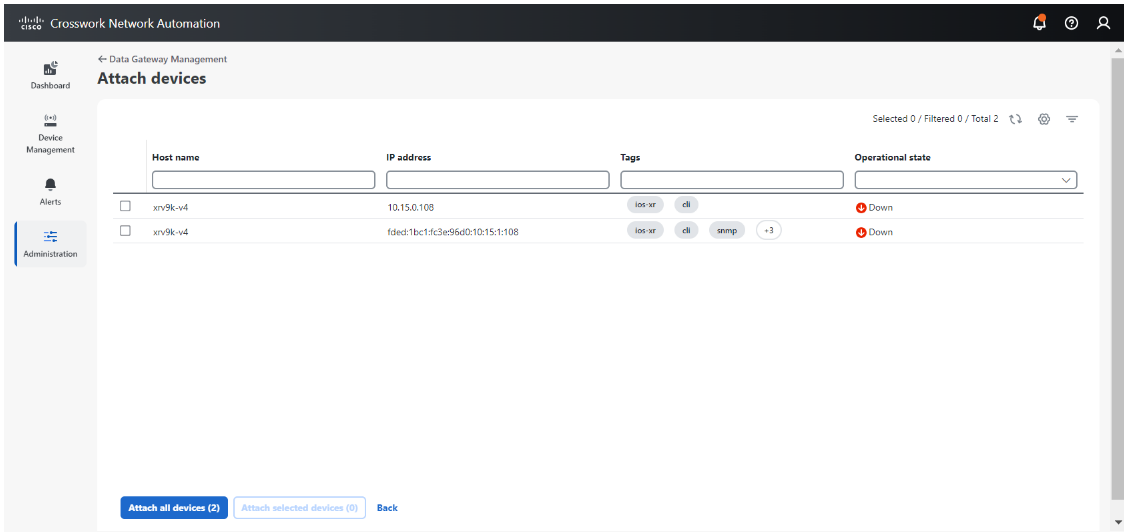
Verify that you are familiar with the prequsites to successfully attach the devices to the Data Gateway. For more information, see Requirement: Device assignment prerequisites.

Procedure

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

Step 2 For the Crosswork Data Gateway where you want to attach devices, select **Actions** > **Attach devices**.

Figure 12: Attach devices



Crosswork Network Automation
Dashboard
Device Management
Alerts
Administration
← Data Gateway Management

Attach devices

Selected 0 / Filtered 0 / Total 2

	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

Attach all devices (2)
Attach selected devices (0)
Back

The **Attach devices** window displays all available devices. In the **Tags** column, if tags are hidden, the UI displays the number of hidden tags. To view these tags, hover over the number (for example, **+3**).

Step 3 To attach all devices, select **Attach all devices**. Or, select individual devices to attach and choose **Attach selected devices**.

Step 4 In the confirmation dialog, select **Attach**.

The selected devices are now associated with the Data Gateway for secure, centralized data collection.

What to do next

- Check the Attached device count in the Data gateways pane to verify your changes.
- Monitor the Data Gateway's health to ensure proper operation with the newly attached devices. For monitoring steps, see *Monitor the Data Gateway health*.

Move devices to a different Data Gateway

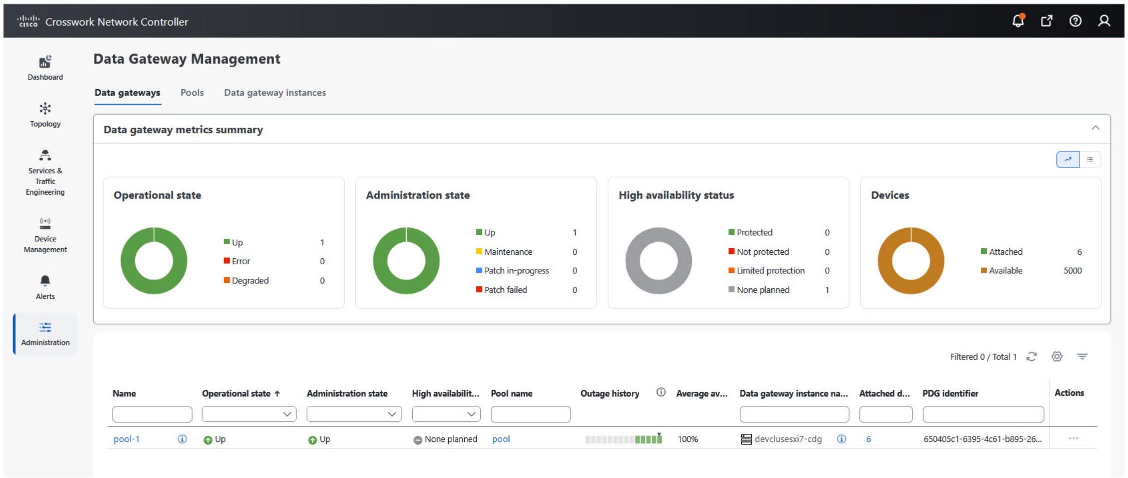
Before you begin

Confirm that you are familiar with the prerequisites required to move devices between Data Gateways. For more information, see Requirement: Device assignment prerequisites.

Procedure

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

Figure 13: Data gateways



Operational state	
Up	1
Error	0
Degraded	0

Administration state	
Up	1
Maintenance	0
Patch in-progress	0
Patch failed	0

High availability status	
Protected	0
Not protected	0
Limited protection	0
None planned	1

Devices	
Attached	6
Available	5000

Filtered 0 / Total 1

Name	Operational state ↑	Administration state	High availabilit...	Pool name	Outage history	Average av...	Data gateway instance na...	Attached d...	PDG identifier	Actions
pool-1	Up	Up	None planned	pool		100%	devclusesxi7-cdg	6	650405c1-6395-4c61-b895-26...	···

Step 2 From the **To this data gateway** drop down, select the Data Gateway to which you want to move the devices.
The Attach devices window lists all available devices.

Step 3 To move all the devices, click **Move all devices**. Otherwise, select the devices you want to move and click **Move selected devices**.

Step 4 In the **Confirm - Move devices** window, click **Move**.

Detach devices from Data Gateway

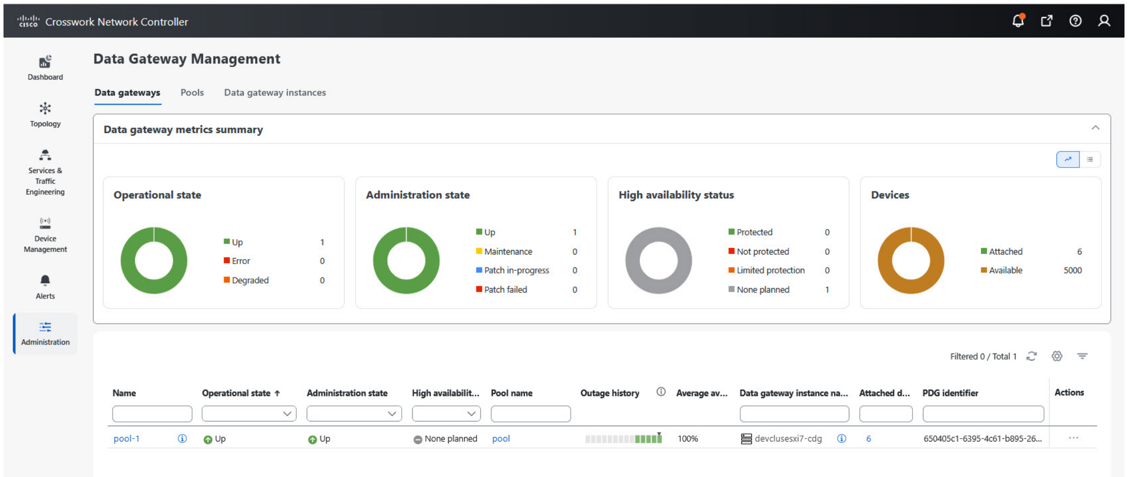
Before you begin

Confirm that you are familiar with the prerequisites required to detach devices from the Data Gateway. For more information, see Requirement: Device assignment prerequisites.

Procedure

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

Figure 14: Data gateways



Operational state	
🟩 Up	1
🟥 Error	0
🟧 Degraded	0

Administration state	
🟩 Up	1
🟨 Maintenance	0
🟦 Patch in-progress	0
🟥 Patch failed	0

High availability status	
🟩 Protected	0
🟥 Not protected	0
🟧 Limited protection	0
⬜ None planned	1

Devices	
🟩 Attached	6
🟧 Available	5000

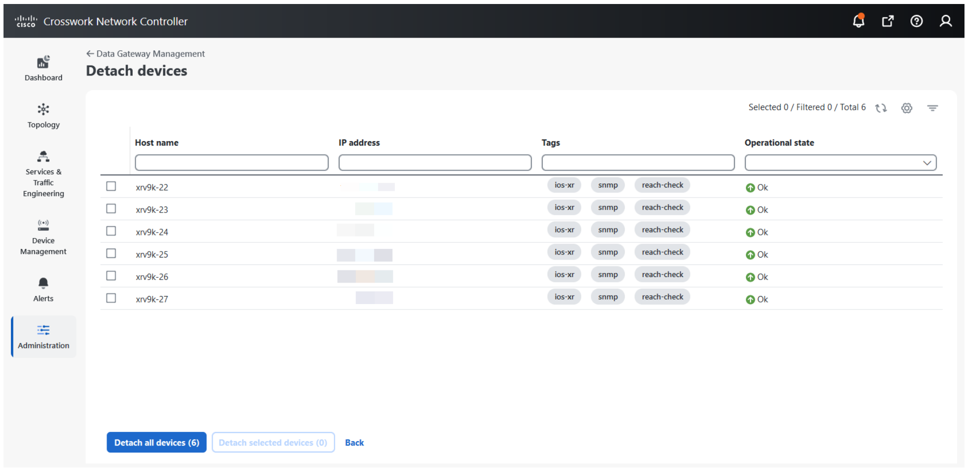
Filtered 0 / Total 1

Name	Operational state ↑	Administration state	High availabilit...	Pool name	Outage history	Average av...	Data gateway instance na...	Attached d...	PDG identifier	Actions
pool-1	Up	Up	None planned	pool		100%	devclusesxi7-cdg	6	650405c1-6395-4c61-b895-26...	⋯

Step 2 For the Data Gateway you want to detach devices from, click the **Actions** column, then click ⋯ and select **Detach devices**.

The **Detach devices** window displays all attached devices.

Figure 15: Detach devices


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

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

Step 3 To detach all devices, click **Detach all devices**. To detach specific devices, select the devices you want, and then click **Detach**.

Step 4 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 ⓘ next to the attached device count to view the list of devices attached to the selected Data Gateway."

For information about initiating a failover, see Perform a manual failover, on page 20.

Delete the Data Gateway instance from Crosswork Network Controller

Remove a Data Gateway instance that is no longer needed.

Use this task when you need to decommission or replace a Data Gateway instance in Crosswork Network Controller.

Before you begin

Review these guidelines to prevent interruptions during the Data Gateway deletion process:

- To prevent collection job loss, move the attached devices to an alternative Data Gateway. If you detach the devices from the Crosswork Data Gateway instance, the corresponding jobs will be deleted.
- If the Data Gateway instance is part of a pool, ensure that it is in the unassigned state.

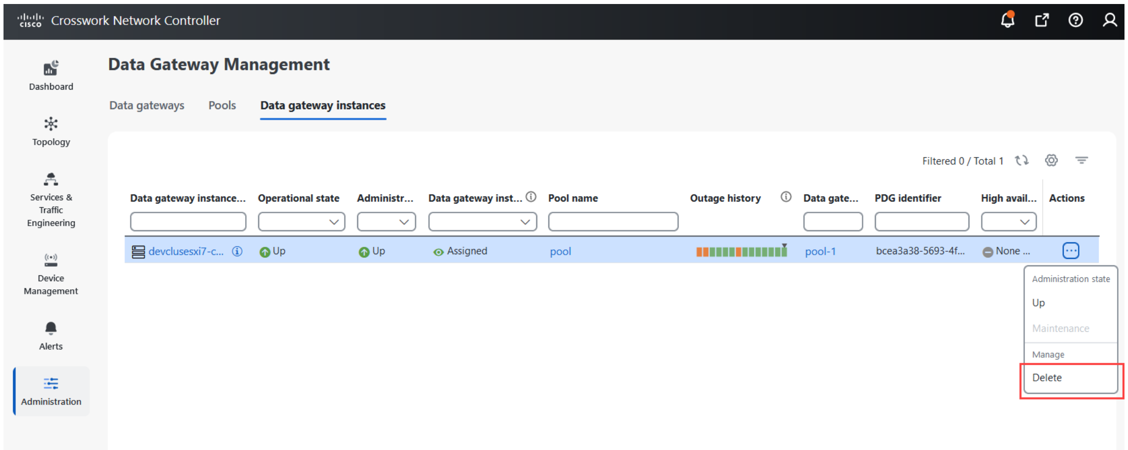
Use these steps to delete the Data Gateway instance from Crosswork Network Controller.

Procedure

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

Step 2 Select the Data Gateway instance you want to delete, click **Delete** under **Actions**.

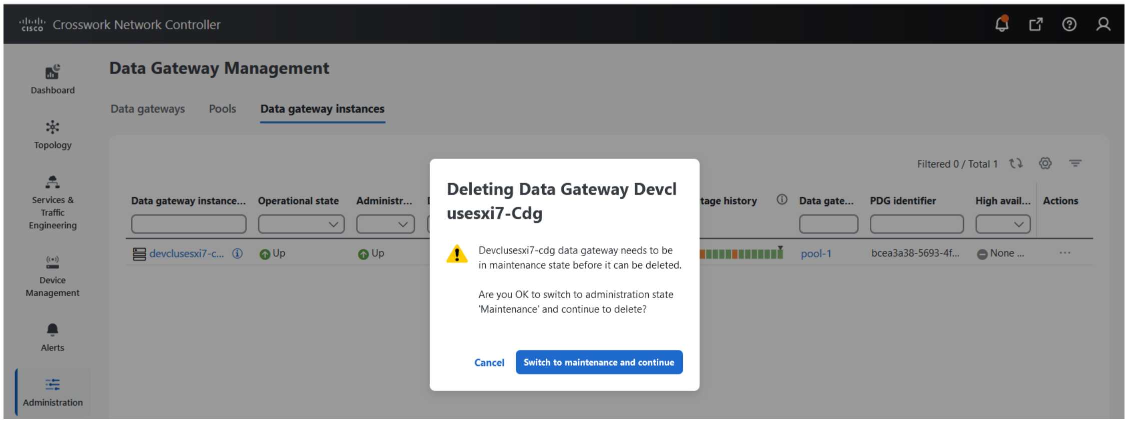
Figure 16: Data Gateway instances



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 If prompted, switch the Data Gateway instance to maintenance mode by clicking **Switch to maintenance & continue**.

Figure 17: Switch to maintenance mode confirmation message



Deleting Data Gateway Devclusesxi7-Cdg

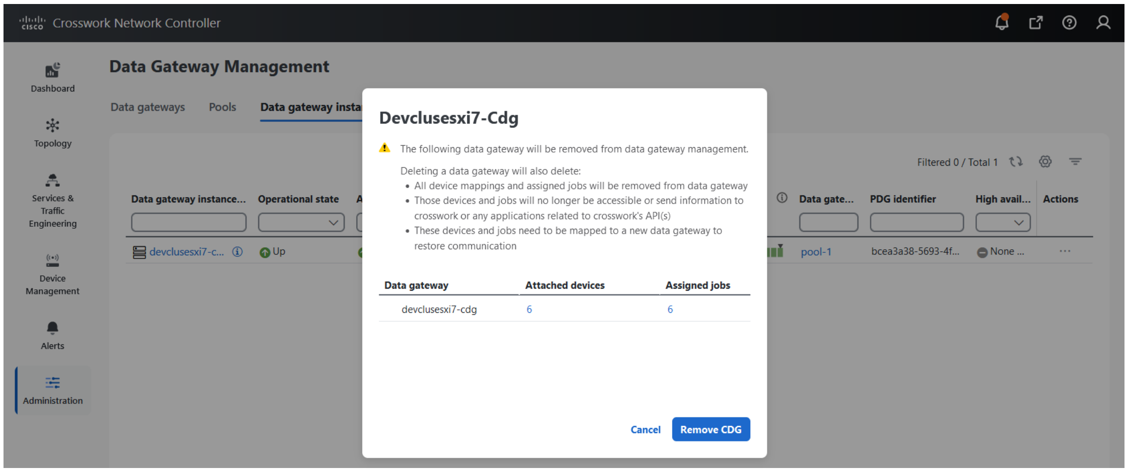
Devclusesxi7-cdg data gateway needs to be in maintenance state before it can be deleted.

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

Cancel | Switch to maintenance and continue

Step 4 Acknowledge the deletion concern by selecting the checkbox, then click **Remove CDG**.

Figure 18: Delete Data Gateway confirmation message



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

The selected Data Gateway instance is removed from Crosswork Network Controller.

What to do next

Verify that all device associations and jobs are redirected or handled by the remaining Data Gateways.

Redeploy a Data Gateway VM

Redeploy a Data Gateway VM in scenarios where the existing VM has gone down and can no longer be used, or when there is a need to change the deployment profile of the VM

Use this task when you need to redeploy a Data Gateway in Crosswork Network Controller.

Before you begin

Review these guidelines to prevent interruptions during the Data Gateway VM redeployment.

- If the Data Gateway VM was already enrolled with Cisco Crosswork and you have installed the VM again with the same name, change the Administration state of the Data Gateway VM to Maintenance for auto-enrollment to go through.
- If a Data Gateway VM was already enrolled with Cisco Crosswork and Cisco Crosswork was installed again, re-enroll the existing Data Gateway VM with Cisco Crosswork. See *Re-enroll Crosswork Data Gateway*.
- If you are redeploying a Data Gateway VM with the same hostname, clear the existing alarms for that hostname to avoid confusion. Old alarms remain viewable in the history. To avoid misunderstanding, check the timestamps on the alarms. This lets you determine whether the alarms were raised on the older Data Gateway or the current one with the same hostname.

Procedure

Step 1 Remove the current Data Gateway VM before installing the new one.

Step 2 Install Data Gateway on the new VM.

For detailed installation instructions, see the *Cisco Crosswork Network Controller 7.2 Installation Guide*.

Step 3 If the redeployment is to change the VM profile, for example, from Standard to Extended, manually roll back any global parameter changes made to the Data Gateway before starting redeployment to avoid configuration conflicts.

Maintenance and post-setup operations

Enable secure, efficient, and interruption-minimized network data collection management by planning downtime, updating configurations, and ensuring proper setup of collections and systems integration. The maintenance activities involve:

- View the Data Gateway alarms, on page 30
- Download the showtech logs, on page 105
- Download service metrics, on page 33
- Reboot Data Gateway VM, on page 34

Crosswork Data Gateway health metrics

A Crosswork Data Gateway health metric is managed from the Data Gateway page that

- indicates the operational state and resource performance of a Data Gateway
- enables historical tracking of outages, performance trends, and possible failures, and
- supports analysis of resource usage such as CPU, network traffic, and service status.

For information on accesing the Data Gateway page, see Access Data Gateway health information (Task).

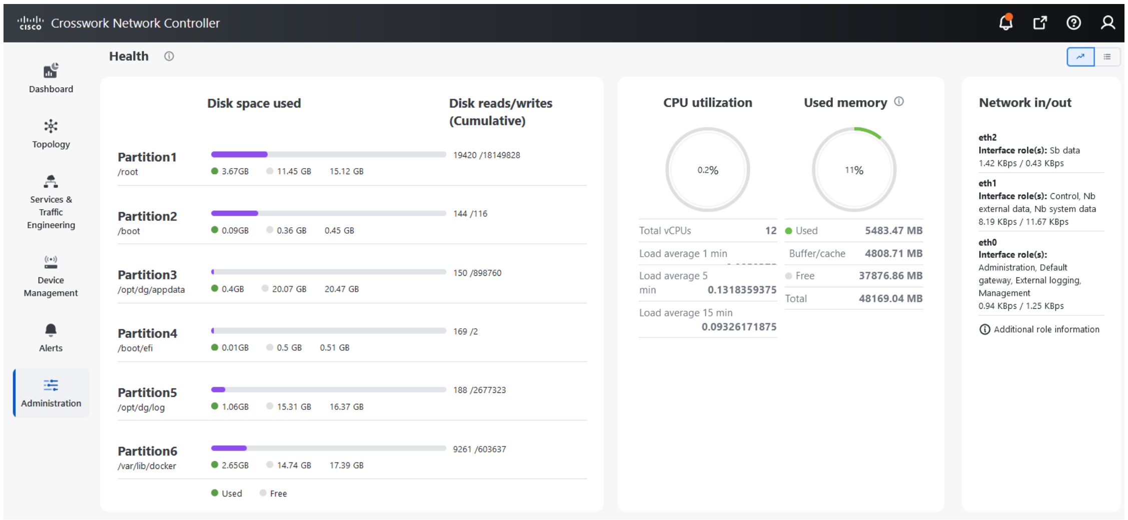
Key metrics and diagnostic tools

These parameters are displayed on the Data Gateway page:

- General Crosswork Data Gateway details: displays the operational state, high availability state, attached device count, and assigned jobs.
- Actions: lists the various troubleshooting options that are available from the UI.
    - Ping: checks the reachability to any IP address.
    - Trace route: helps troubleshoot latency issues. This option provides 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, such as collectors (cli-collector) and infra services (oam-manager). Log level changes apply only to the Data Gateway receiving the change.
- History: shows the outage chart for Data Gateway over 14 days. The chart includes timestamps, outage times, and clear times.

    The top-right corner of the pane provides options to zoom in, zoom out, pan, or download the history chart as SVG or PNG files for specific time periods.
- Events: lists state changes, role changes, reason messages, timestamp, and duration over the last 14 days.
- Health: indicates health information, last health data collected, error states, CPU utilization alerts, and NIC traffic speeds.
    - 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 it increases further, which could lead to failure of the Data Gateway.
    - The Network In/Out section displays the speed at which the vNICs send and receive network data.
    - To view the interface roles assigned to the vNICs, click the ? icon next to Additional role information. The popup provides information about the available roles.

Figure 19: Crosswork Data Gateway health



Health

	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 health information for each container service running on the Data Gateway, as well as resource consumption. For any individual service, you can restart it using Actions > Restart. The Load column shows the processing load of each collector or service. Load scores are calculated using several metrics and mapped to low, medium, or high severity zones.

  A collector that consistently operates in the High zone has reached peak capacity for its assigned CPU or memory resource profile. For more information on load score calculation, see Load Score Calculation.

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

Note The list of container services differs between Standard Data Gateway and Extended Data Gateway, with the Extended Data Gateway having more containers installed.

View the Data Gateway alarms

Identify and review Data Gateway alarms indicating anomalies in data collection.

Use this task to monitor for issues that prevent data collection and determine appropriate remediation actions.

Before you begin

- Ensure that the Data Gateway for which you want to view the alarms is registered and operational.
- Verify that the alarm pod status is healthy.

Use these steps to review the alarms to understand the issue affecting data collection, and take the remediation action, if necessary. Alternatively, you can log in to the alarms pod and view the alarms in the DgManager.yaml file.

Procedure

Step 1 Navigate to **Administration** > **Crosswork Manager** > **Application Management** tab and then select **Applications**.

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

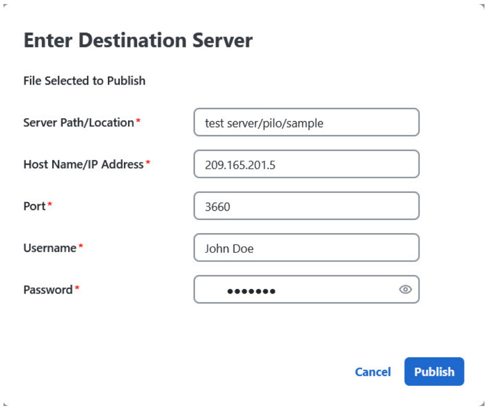
Step 3 In the Microservices tab, filter by "alarms" to locate the alarm pod.

Step 4 To view alarm details, select **Showtech requests** under **Actions**.

Step 5 Review the information displayed in the **Showtech Requests** window.

Step 6 To export alarm logs, choose **Publish** and enter the destination server details.

Figure 20: Edit destination servers



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* •••••••

Data Gateway alarms are displayed for review. You can download logs for further analysis and remediation.

What to do next

If an alarm indicates an issue, perform the recommended remediation action.

Download the showtech logs

Collect diagnostic logs from a specific Data Gateway for troubleshooting and support.

Use this procedure to download encrypted showtech logs from Crosswork Network Controller for a selected Data Gateway.

Note Showtech logs cannot be collected from the UI if the data gateway is in an ERROR state. In the DEGRADED state, if the OAM-Manager service is operational and not degraded, logs can be collected.

Before you begin

Confirm that the Data Gateway is not in ERROR state. If the gateway is in DEGRADED state and the OAM-Manager service is running and not degraded, logs may still be collected.

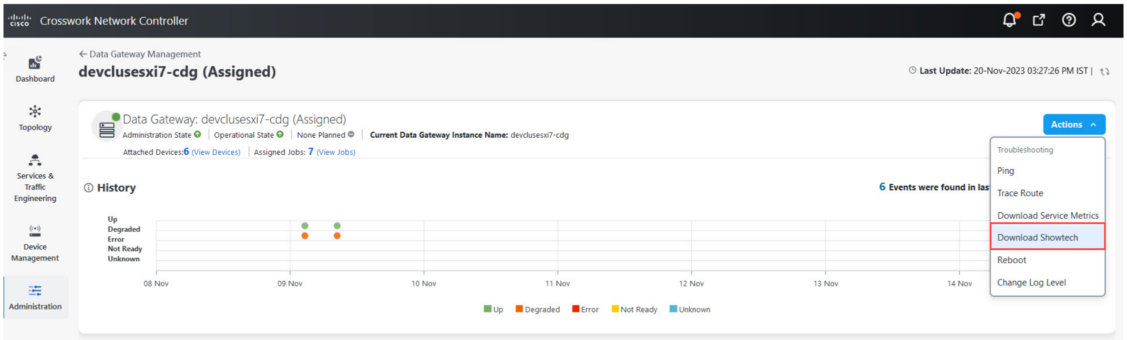
Procedure

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

Step 2 Select the relevant Data Gateway.

Step 3 In the details page, click Actions and choose **Download Showtech**.

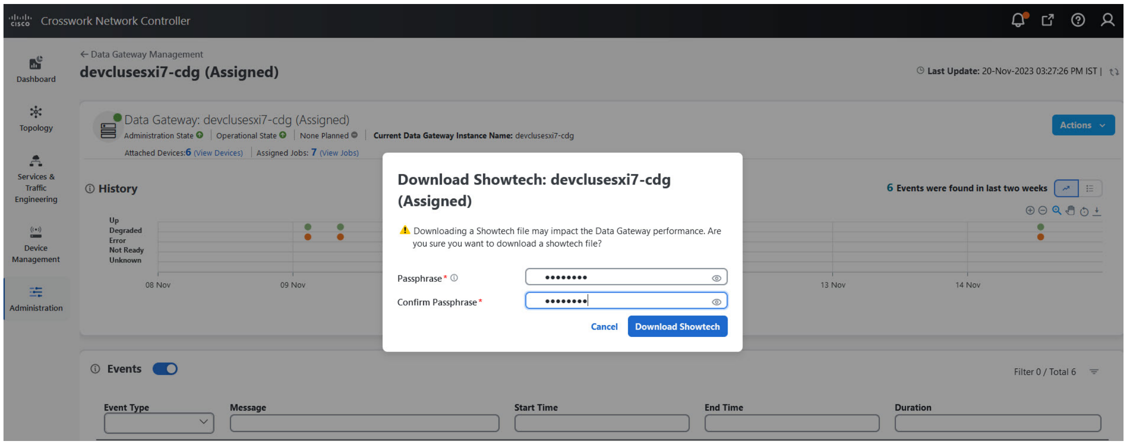
Figure 21: Download showtech


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
Up
Degraded
Error
Not Ready
Unknown
Troubleshooting
Ping
Trace Route
Download Service Metrics
Download Showtech
Reboot
Change Log Level

Step 4 Enter the desired passphrase.

Make a note of this passphrase because it is required to decrypt the downloaded file.

Figure 22: Download Showtech pop-up


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
Cancel
Download Showtech

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 * ••••••••

Step 5 Click **Download Showtech**.

The logs are downloaded in encrypted format.

Note
The download time depends on system usage.

Step 6 After the download completes, decrypt the file using the command:

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<password>
```

Example:

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in show-tech-file.tar.xz.enc -out
show-tech-file.tar.xz -pass pass: myPassword
```

- Use OpenSSL version 1.1.1i to decrypt the file. To check the OpenSSL version on your system, use the command `openssl version` .
- The `<showtech file>` must have a `.tar.xz` extension.
- Do not use quotation marks for filenames.
- On a Mac operating system, use OpenSSL 1.1.1+ since LibreSSL is not supported.

The decrypted showtech file is available for analysis or to send to support.

What to do next

- Securely store the decrypted log file.
- Provide the file to support as needed.

Download service metrics

Download and decrypt service metrics for data gateway instances from the Crosswork UI.

Use this procedure to retrieve encrypted metrics files for all collection jobs from a Data Gateway for analysis or troubleshooting.

Before you begin

Ensure that you meet these requirements during decryption:

- Use OpenSSL version 1.1.1i or newer. To check, use `openssl version`.
- On a Mac, ensure that you are not using LibreSSL, as it does not support the necessary switches.
- The metrics file must have a `.tar.xz` extension.

Procedure

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 **Data Gateway details** page, on the top-right corner, click **Actions** > **Download Service Metrics**.

Step 4 Enter a passphrase.

Note
Make a note of this passphrase because you will use it later to decrypt the file.

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

Step 6 After the download, decrypt the file using the OpenSSL command.

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<password>
```

Example:

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in show-tech-file.tar.xz.enc -out
show-tech-file.tar.xz -pass pass: myPassword
```

- Do not enclose filenames in quotation marks when running the command.
- Use OpenSSL version 1.1.1i to decrypt the file. To check the OpenSSL version on your system, use the command `openssl version`.
- The `<showtech file>` must have a `.tar.xz` extension.
- Do not use quotation marks for filenames.
- On a Mac operating system, use OpenSSL 1.1.1+ since LibreSSL is not supported.

The decrypted metrics file is available for use or analysis.

Reboot Data Gateway VM

Restart a data gateway virtual machine to restore or refresh its services.

Perform this task from the Crosswork Network Controller UI. When you reboot the data gateway, its functionality is paused until the VM is running again.

Before you begin

Be aware that rebooting the Data Gateway pauses its functionality until the virtual machine restarts.

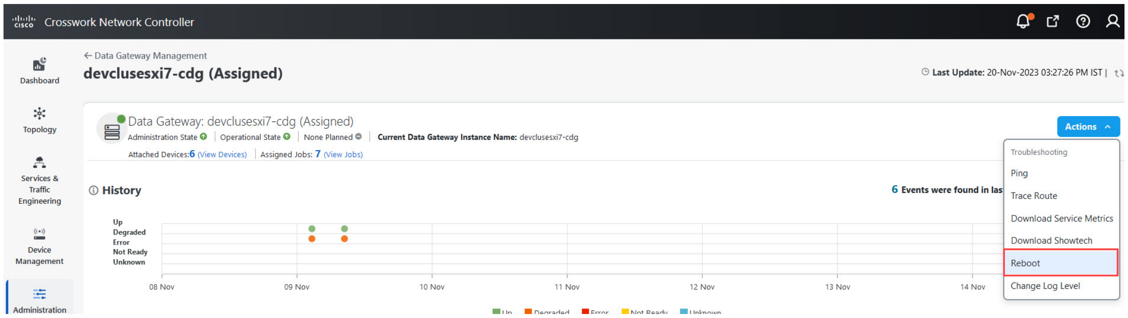
Procedure

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

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

Step 3 On the **Crosswork Data Gateway details** page, at the top-right, click **Actions**, then click **Reboot**.

Figure 23: Data Gateway reboot



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

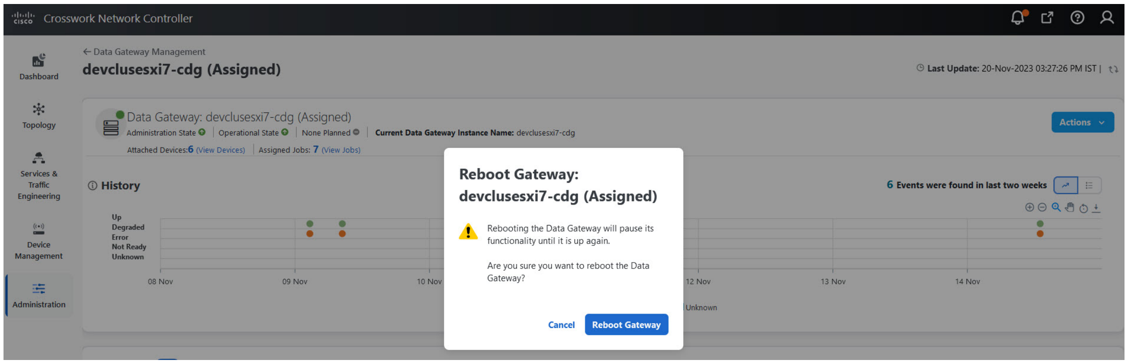
Attached Devices:6 (View Devices) | Assigned Jobs: 7 (View Jobs)

History

6 Events were found in las

Step 4 Click **Reboot Gateway** to confirm.

Figure 24: Reboot Data Gateway pop-up



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?

Cancel | Reboot Gateway

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

Global settings and resource allocation

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

- Configure the global Data Gateway settings, on page 35
- Allocate the Data Gateway resources , on page 37
- Enable or disable collectors, on page 38

Configure the global Data Gateway settings

You can update global parameters on all Crosswork Data Gateways in the network using Crosswork Data Gateway.

Before you begin

nsure that you are aware of these points:

- Only an admin user can access these settings.
- Familiarize with the parameters that you would be configuring. See Data Gateway global parameters, on page 36.
- Confirm that you are aware of the guidelines to update the ports. See Guidelines for updating port values, on page 36.

Procedure

Step 1 Go to **Administration** > **Data Collector(s) Global Settings** > **Global parameters**.

Step 2 Change the required global parameters.

For information about the parameters, see Data Gateway global parameters, on page 36.

Step 3 Select **Yes** in the **Global parameters** window if you're updating ports.

For information on port update guidance, see Guidelines for updating port values, on page 36.

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 may get restarted as part of the recovery.

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**.

Guidelines for updating port values

To properly update port values, you must:

- Confirm that the port values you want to update are valid ports.
- Check that the new port values don’t conflict with existing ones on the Crosswork Data Gateway.
- Configure the same port values on the device.
- Restart the collectors and pause any in-progress collection jobs to update ports.
- After the restart is complete, collection jobs will resume automatically.

Data Gateway global parameters

This table lists and describes the parameters required for configuring the Data Gateway.

Table 4: Parameters and descriptions

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

Parameter name	Description	Default value for cluster VM deployment
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 5–900 seconds
SNMP trap port	Adjust the value according to your deployment environment and configuration requirements.	1062 Accepted range is 1–65535
Syslog UDP port	Adjust the value according to your deployment environment and configuration requirements.	9514 Accepted range is 1–65535
Syslog TCP port	-	9898 Accepted range is 1–65535
Syslog TLS port	-	6514 Accepted range is 1–65535
Re-Sync SNMPv3 details	The 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.	Disable By default, this option is disabled for security reasons. Automatic synchronization of updated User Security Model (USM) information is not permitted to prevent unintended data collection from an incorrect source. When enabled, the system automatically updates USM information after changes, such as hardware updates or device reboots. This ensures that data collection continues without user intervention. If the option remains disabled, manually intervene to re-establish USM communication. This can be done by either detaching and reattaching the device to the Crosswork Data Gateway pool or toggling the device's admin state as Down and then Up.

Allocate the Data Gateway resources

Crosswork Data Gateway allows you to dynamically configure and allocate memory at runtime for collector services.

You can allocate more memory to a heavily used collector or adjust the balance of resources from the UI.

Before you begin

Ensure that you are aware of these points.

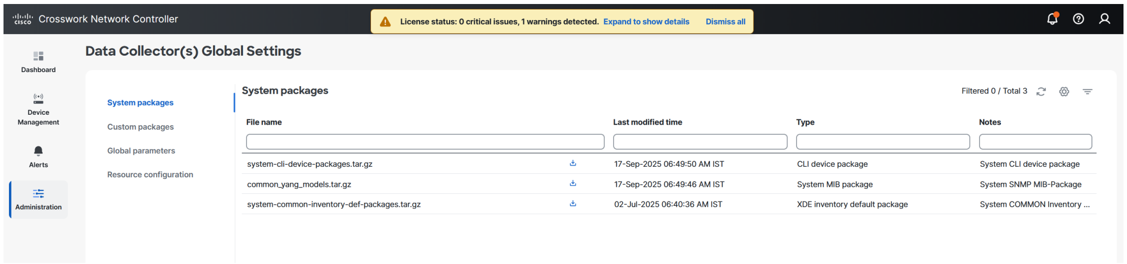
- The **Resource configuration** page displays the memory currently configured for collector services. Changes to the memory values apply to both currently enrolled and future Crosswork Data Gateways.
- The list of collectors displayed on this page is dynamic; it is specific to the deployment.
- Update resource allocation for collectors only if you are working with the Cisco Customer Experience team.
- When you update the values for a collector, the collector restarts and pauses any collection jobs that are running.
- The NETCONF data collection support is deprecated starting from the Crosswork Network Controller 6.0 release.

Use these steps to dynamically configure and allocate memory at run time for collector services.

Procedure

Step 1

Figure 25: Resource configuration



License status: 0 critical issues, 1 warnings detected. Expand to show details Dismiss all

Data Collector(s) Global Settings

System packages

File name	Last modified time	Type	Notes
system-cli-device-packages.tar.gz	17-Sep-2025 06:49:50 AM IST	CLI device package	System CLI device package
common_yang_models.tar.gz	17-Sep-2025 06:49:46 AM IST	System MIB package	System SNMP MIB-Package
system-common-inventory-def-packages.tar.gz	02-Jul-2025 06:40:36 AM IST	XDE inventory default package	System COMMON Inventory ...

Step 2 Enter the updated values in the **Memory** field for the collectors you want to update.

Attention
We recommend a minimum memory size of 2,000 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**.

Enable or disable collectors

Manage collector services to optimize resource usage or resolve collector-related issues.

Crosswork Data Gateway uses configured collectors to gather device data. You may need to enable or disable collectors to optimize resource allocation or when troubleshooting collector-related problems.

Before you begin

Review this information before enabling or disabling a collector:

- SNMP and CLI collectors cannot be disabled, as they are required for device reachability.

- By default, all collectors are enabled.
- Disable collectors only during Day 0 or Day 1 configuration. If you want to disable a collector after Day 1, the administrator must manually clear the associated collection jobs.
- The NETCONF data collection support is deprecated starting from the Crosswork Network Controller 6.0 release.

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.

Procedure

Step 1 Go to **Administration** > **Data Collector(s) Global Settings** > **Resource configuration**.

The list of collectors and the resource limits is displayed.

Step 2 Review the list of collectors and their resource limits.

Step 3 For each applicable collector, select the **Enable collector** check box to enable data collection, or clear the check box to disable it.

Step 4 Click **Save**.

Your selections determine whether collector services are enabled or disabled. Set memory utilization for each collector as needed. To learn more about resource allocation, see Allocate the Data Gateway resources , on page 37.

External data destinations

An external data destination is a configurable endpoint that allows you to:

- receive data from Crosswork Data Gateway collection jobs and applications
- support integration with platforms like Kafka or external gRPC, and
- allow management through Crosswork Network Controller interface.

Characteristics of external data destinations

Each data destination has a unique identifier (UUID), which is automatically generated by Crosswork Network Controller when a destination is created.

- When creating collection jobs via the Crosswork Network Controller UI, select the destination from a drop-down list of configured destinations.
- When creating a collection job via the API, use the UUID of the destination the collector should send data to.

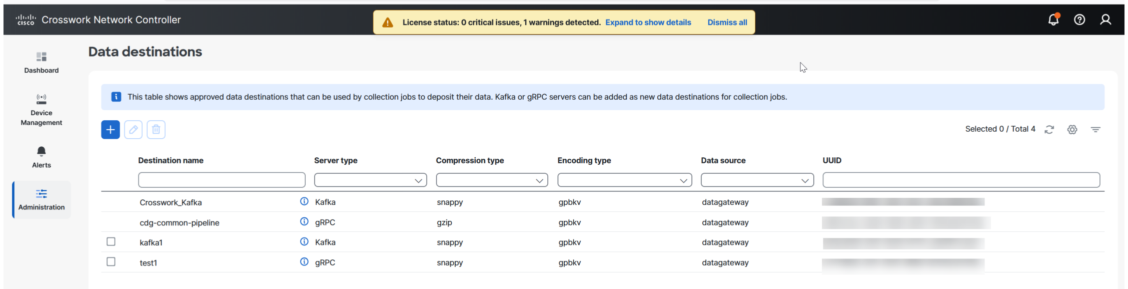
The **Data destinations** page allows users to:

- add new data destinations
- update settings for existing data destinations, and
- delete data destinations.

The **Data destinations** page displays all approved data destinations that collection jobs can use to deposit data.

To view details of a data destination in the **Data destinations** page, click ? next to the name of the data destination you want to view.

Figure 26: Data destinations



Crosswork Network Controller
License status: 0 critical issues, 1 warnings detected. Expand to show details Dismiss all
Dashboard
Device Management
Alerts
Administration
Selected 0 / Total 4

Data destinations

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	Data source	UUID
	Crosswork_Kafka	Kafka	snappy	gpbkv	datagateway	[redacted]
	cdg-common-pipeline	gRPC	gzip	gpbkv	datagateway	[redacted]
□	kafka1	Kafka	snappy	gpbkv	datagateway	[redacted]
□	test1	gRPC	snappy	gpbkv	datagateway	[redacted]

Add or edit a data destination

Use these steps to add or edit a data destination:

Procedure

Step 1 Access the data destination configuration:

a) Go to **Administration** > **Data Destinations**.

Step 2 Add or edit a destination:

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

a) To add a new destination, click **Add New Destination** and fill in the required fields.

b) To edit an existing destination, click the ✎ icon.

Step 3 Enter the required destination details. For information about the fields, see Parameters for configuring data destinations, on page 44.

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 If you selected **Data Gateway** or **Any** as the data source and the server is set to **Kafka**, you can configure custom values for individual collectors when needed. To override the global properties for a Kafka destination, use the settings in the **Destination – Per Collector Properties** pane.

a) Select a **Collector**.

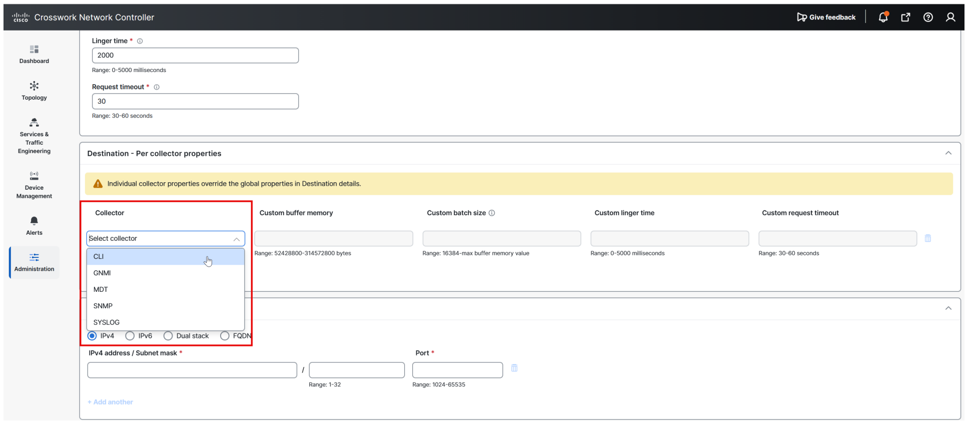
b) Enter the values as:

- **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 27: Add destination



Linger time *
2000
Range: 0-5000 milliseconds

Request timeout *
30
Range: 30-60 seconds

Destination - Per collector properties

Individual collector properties override the global properties in Destination details.

Collector	Custom buffer memory	Custom batch size	Custom linger time	Custom request timeout
Select collector	Range: 52428800-314572800 bytes	Range: 16384-max buffer memory value	Range: 0-5000 milliseconds	Range: 30-60 seconds

● IPv4 ○ IPv6 ○ Dual stack ○ FQDN

IPv4 address / Subnet mask * /
Range: 1-32
Port *
Range: 1024-65535

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 the protocol and host details in the **Connection details** sections. The supported protocols are IPv4, IPv6, dual stack, and FQDN. For information about the accepted range, see Parameters for configuring data destinations, on page 44.

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. For information about the connection details, see Parameters for configuring data destinations, on page 44.

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

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) Enable security configurations.

a) If the data source is set to Data Gateway, the **Enable secure communication** check box is displayed. To connect securely to a Kafka or gRPC-based data destination, select this check box. Then select the type of authentication process from the available options.

- **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. **Mutual-Auth** is the default authentication process.

  Note
  Crosswork supports mutual authentication only for destinations with the data source set to **Application** or **Any**.

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

b) If the data source is set to **Any** or **Application**, the **Enable secure communication with mutual auth** check box is displayed. Select this check box to enable the security feature.

Step 8 Click **Save**.

What to do next

1. This step applies if you have selected the data source as **Data Gateway** or **Any**.

   Create the required Kafka topics:

   - Configure the Kafka destination with the `reachability-topic` before initiating a new collection job. This is required for health monitoring of the destination.

   - The topics must exist in the external Kafka at the time of data dispatch; otherwise, Crosswork logs may display an exception:

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

2. If you have enabled secure communication when adding the destination, go to the **Certificate Management** page in the 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 Overview for more information.

Important When the data source is set to **Data Gateway** or **Any**, a missing or incomplete certificate causes the destination to enter an error state. The associated collection job is marked as **Degraded**. For details about certificate requirements and management, see your platform's certificate management documentation.

Requirement to prepare external servers for data destination

To use an external Kafka server as a data destination in Crosswork Data Gateway, ensure these requirements are met:

- Determine the data source for your destination as Data Gateway or application (Element Management Function, Service Health, and so on). If you are unsure, you can select **Any**. The form shows or hides specific fields depending on the selected data source. For example, encoding types and security details. Be prepared to provide the fields that apply to your chosen source.
- Configure the external Kafka server with these properties:
  - num.io.threads = 8
  - num.network.threads = 3
  - message.max.bytes = 30000000

  Refer to the official Kafka documentation for details on these property configurations.
- Confirm that the external Kafka server is reachable and that port connectivity is properly established.
- If security is enabled, provide certificates in PEM-encoded format and use PKCS#8 format for key files.
- For client authentication, ensure the required certificate, key files, and password (if necessary) are available.
- Use the same IP protocol (IPv4 or IPv6) on the external destination as specified during the Crosswork Network Controller deployment.

Best practice for adding external data destinations

When configuring an external data destination like a Kafka server, consider these behaviors and practices:

- If you reinstall an existing Kafka destination using the same IP address, restart collectors for the changes to take effect.
- Secure the communication channel between the management system and the destination; enabling security may impact performance.

Note Enabling security may impact performance.

- If the external destination requires TLS, prepare these configurations in advance:
  - Public certificate for server authentication
  - Client certificate and key files for mutual authentication
  - If the client key is password-encrypted, configure the password during data destination provisioning.
- Verify port connectivity for the external destination; if unreachable, data collection fails.
- Configure custom values for a Kafka destination in the destination properties; this is not supported for gRPC destinations.

- Mandatory global properties specified in the Destination Details panel apply to all Kafka destinations, but collector-level custom values override them for that collector.
- Match the IP version (IPv4 or IPv6) between the external destination and the deployment settings.
- Changes to hostname-to-IP mappings only take effect after the DNS TTL expires; to apply changes immediately, reboot the VM.

Parameters for configuring data destinations

These tables list and describe the parameters required for adding or editing the data destinations.

Table 5: Parameters and their descriptions

Parameters	Description	Available in gRPC	Available in Kafka
Destination name	Enter a descriptive name (up to 128 characters). Valid characters include letters, numbers, hyphens (-), underscores (_), and periods (.). Avoid all other special characters. If you have many data destinations, choose an informative name to allow for easier identification later.	Yes	Yes

Parameters	Description	Available in gRPC	Available in Kafka
Data source		Yes	Yes

Parameters	Description	Available in gRPC	Available in Kafka
	Identifies which Crosswork component or application will use the external Kafka or gRPC destination to send data. This field determines the available configuration options, validation rules, and security features for the destination. Select one of the data sources • **Data Gateway**: destination exclusively used by Crosswork Data Gateway for telemetry and network data collection. • **Application**: destination exclusively used by Crosswork applications for data such as alarms, inventory notifications, performance monitoring. The application could be Element Management Function or Crosswork Optimization Engine. • **Any**: destination can be shared by both **Data Gateway** and **Applications**. **Note** • If you do not choose the data source, it defaults to **Data Gateway**. • If you set the data source to **Any**, you cannot change it later. To select a different data source, delete the destination and create a new one. • When you change the data source from **Data Gateway** to **Any** during editing a destination, Crosswork automatically switches the authentication type to mutual authentication and displays a warning message. • Crosswork Data Gateway does not monitor the availability of Kafka destinations configured with the dispatch source as **Application** (Dispatch Source="application"). If a destination becomes unreachable, applications such as Service Health fail to detect the issue or notify users, which can result in silent data loss. • When upgrading from Crosswork 7.1 or earlier, all destinations default to **Data**		

Parameters	Description	Available in gRPC	Available in Kafka
	Gateway. • Destinations that have **Application** as the data source are removed after the upgrade.		
Server type	Select the server type as Kafka or gRPC of your data destination.	Yes	Yes
Encoding type **Note** This field appears only when the data source is set to Data Gateway or Any.	Choose the compression method as either Json or Gpbkv.	Yes	Yes
Compression method	Choose the desired compression type.	Yes Supported compression types are snappy, gzip, and deflate.	Yes Supported compression types are snappy, gzip, zstd, and none. **Note** zstd compression type is supported only for Kafka 2.0 or higher.
Dispatch type	This parameter is available when the **Server Type** field is set to **gRPC**. Select stream or unary as the dispatch method. By default, unary is used. Crosswork Data Gateway sends the collected data using either data streams or unary transmission.	Yes	No
Maximum message size	Enter the maximum message size in bytes. • Default value: 100000000 bytes/100 MB • Min: 1000000 bytes/1 MB • Max: 100000000 bytes/100 MB	No	Yes

Parameters	Description	Available in gRPC	Available in Kafka
Buffer memory	Enter the buffer memory required, in bytes. • Default value: 52428800 bytes • Min: 52428800 bytes • Max: 314572800 bytes	No	Yes
Batch size	Enter the required batch size in bytes. • Default value: 1048576 bytes/1.048576 MB • Min: 16384 bytes/16.38 KB • Max: 314572800 bytes/6.4 MB	No	Yes
Linger time	Enter the required linger time in milliseconds. • Default value: 2000 ms • Min: 0 ms • Max: 5000 ms	No	Yes
Request timeout	Enter the duration that the request waits for a response. When the configured duration is reached, the request expires. • Default value: 30 ms • Min: 30 ms • Max: 60 ms	No	Yes

Table 6: Connection details

Connectivity Type	Fields	Available in gRPC	Available in Kafka
IPv4	Enter the required IPv4 address, subnet mask, and port. You can add multiple IPv4 addresses by clicking **+Add another**. IPv4 subnet mask ranges from 1 to 32 and port range from 1024 to 65535.	Yes	Yes
IPv6	Enter the required **IPv6 address/Subnet mask**, and **Port**. You can add multiple IPv6 addresses by clicking **+Add another**. IPv6 subnet mask ranges from 1 to 128.	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**. IPv4 subnet mask ranges from 1 to 32 and port range from 1024 to 65535. IPv6 subnet mask ranges from 1 to 128. **Note** The Dual Stack option is available only when your system supports this configuration.	Yes	Yes
FQDN	Enter the required **Host name**, **Domain name**, and **Port**. The supported port range is from 1024 to 65535. You can add multiple FQDN addresses by clicking **+ Add another**.	Yes	Yes

Delete a data destination

Remove data destinations that are no longer required for data gateway configuration.

Delete a data destination to remove outdated or unused endpoints from your Data Gateway settings. Default destinations, such as `Crosswork_Kafka`, cannot be deleted.

Procedure

Step 1 Go to **Administration** > **Data destinations**.

Step 2 Select the data destinations you want to remove.

Step 3 Delete the selected destinations.

When prompted, confirm the deletion.

The selected data destinations are removed from your configuration and the corresponding data subscriptions are also deleted.

What to do next

Review the configuration to confirm that no necessary data destinations have been deleted by mistake.

Subscription APIs

After configuring data destinations, data subscriptions must be created to define what data gets sent where. Data subscription types include data such as alarms, inventory changes and performance metrics.

API endpoint: `POST /crosswork/notification/v2/subscription`

API details

```
*destinationName*: Name of an existing data destination
*destinationType*: Type of destination ('Kafka' or 'gRPC')
*subscriptionDataType*: Type of data subscription
  -  Possible types for Kafka: Inventory_Changes, Alarm, System_Audit,
Device_Performance_Monitoring, Network_Performance_Monitoring, Service_Health_Monitoring
  -  Possible types for gRPC: Device_Performance_Monitoring, Network_Performance_Monitoring
*subscriptionData*: policy_instance=performance monitoring policy (Example: Device health
or Interface health)
*topicName*: Kafka or gRPC topic name
*filter*: Optional filter criteria applicable only for Inventory_Changes data type (set to
 'null' if not required)
```

A success response is returned when the request is completed.

Subscription validation criteria

Successful subscription for Kafka or gRPC destination types is validated using a unique combination of the following four parameters:

- `destinationType`e
- `subscriptionDataType`
- `subscriptionData`
- `topicName`

Examples:

- For Kafka:
    - `destinationType`: "Kafka"
    - `subscriptionDataType`: "Service_Health_Monitoring"
    - `subscriptionData`: "PCA_Probes"

      `topicName`: "sh.tracker.topic.PCA_probes"
- For gRPC:
    - `destinationType`: "gRPC"
    - `subscriptionDataType`: "Network_Performance_Monitoring"
    - `subscriptionData`: "SR_PM_Policy"
    - `topicName`: "pmdata-test-grpc-NPM"

A subscription is considered successful only if this parameter combination, along with a unique topic name, is validated.

Sample: Kafka subscription request for alarms

This sample creates a Kafka data subscription for alarm monitoring:

```
POST /crosswork/notification/v2/subscription
{
  "destinationName": "kafka-alarm-destination",
  "destinationType": "Kafka",
  "subscriptionDataType": "Alarm",
  "subscriptionData": null,
  "topicName": "topic_name",
  "filter": null
}
```

Sample: Kafka subscription request for performance monitoring

This sample creates a Kafka data subscription for performance monitoring.

Note `subscriptionData` is applicable only for device performance monitoring subscriptions in Kafka.

```
POST /crosswork/notification/v2/subscription
{
  "destinationName": "kafka-alarm-destination",
  "destinationType": "Kafka",
  "subscriptionDataType": "Device_Performance_Monitoring",
   "subscriptionData": "policy_instance=device_health",
   "topicName": "pm-topic",
   "filter": null
}
```

Sample: gRPC subscription request for device performance monitoring

This sample creates a gRPC data subscription for device performance monitoring:

```
POST /crosswork/notification/v2/subscription
{
  "destinationName": "grpc-device-perf-destination",
  "destinationType": "gRPC",
  "subscriptionDataType": "Device_Performance_Monitoring",
  "subscriptionData": "policy_instance=device_health",
  "topicName": "device-perf-context-001",
  "filter": null
}
```

Sample: gRPC subscription request for network performance monitoring

This sample creates a gRPC data subscription for network performance monitoring:

```
POST /crosswork/notification/v2/subscription
{
"destinationName": "grpc-secure",
"destinationType": "gRPC",
"filter": null,
"subscriptionData": "SR_PM_Policy",
"subscriptionDataType": "Network_Performance_Monitoring",
"topicName": "pmdata-test-grpc-NPM"
}
```

Sample: Service health PCA_probes and Y1731_probes payloads

This sample creates a Service_Health_Monitoring subscription for PCA_probes and Y1731_probes:

```
PCA_probes
{
"destinationName": "kafka-fqdn",
"destinationType": "KAFKA",
"subscriptionDataType": "Service_Health_Monitoring",
"subscriptionData": "PCA_Probes",
"topicName": "sh.tracker.topic.PCA_probes",
"filter": null
}


Y1731_probes
{
"destinationName": "kafka-test",
"destinationType": "KAFKA",
"subscriptionDataType": "Service_Health_Monitoring",
"subscriptionData": "Y1731_Probes",
"topicName": "sh.tracker.topic.Y1731",
"filter": null
}
```

Refer to Crosswork Network Controller APIs for more details about adding an external Kafka or gRPC subscription.

Manage data subscriptions

Use the **Data subscriptions** option to view or delete active Kafka or gRPC subscriptions.

Procedure

Step 1 From the main menu, choose **Administration** > **Users and Roles**.

Step 2 Click **Data subscriptions**.

Step 3 Filter subscriptions by selecting the destination type and data type from the available options.

Step 4 To delete a subscription, choose the subscription you want to remove and click the **Delete** icon.

Device package management

A device management capability, often referred to as device package management, is a feature of Cisco Crosswork Data Gateway that

- extends data collection capabilities to Cisco applications and third-party devices
- supports both custom and system device packages that are pre-bundled and automatically deployed but cannot be modified, and

- allows customization and uploading of device packages to cover third-party devices or specific data collection needs not addressed by default packages, with support available from Cisco or Cisco partners.

Types of custom packages

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

- CLI device package: Use CLI-based KPIs to monitor the health of third-party devices. Include all custom CLI device packages and their corresponding YANG models in the file `custom-cli-device-packages.tar.xz`. The system does not support multiple files. You can use the aggregate package to bundle various files for different devices in a single package.
- Custom MIB package: Custom MIBs and device packages can be specific to third-party devices. They can also be used to filter collected data or format it differently for Cisco devices. You can edit these packages. Include all custom SNMP MIB packages, along with the necessary YANG models, in the file `custom-mib-packages.tar.xz`. The system does not support multiple files.

Note Crosswork Data Gateway enables SNMP polling on third-party devices for standard MIBs included in the system. You only need proprietary MIBs if the collection request references specific table names or scalar names from a proprietary MIB. If the requests are OID-based, MIBs are not required.

- SNMP device package: Extend SNMP coverage by uploading custom SNMP device packages in the .xar format.
- Aggregate package: Include multiple supported file extensions in a single package. These files can be collector or application-specific. For example, an aggregate package can contain files for CLI and SNMP device packages.

Supported file types for custom packages

In the Crosswork UI, you can upload or download device or data collection packages that extend the Data Gateway's coverage or functionality. Each package can include a combination of these file types, depending on whether you are installing custom device definitions, YANG models, or SNMP MIBs.

- 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

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

Summary

Crosswork Network Controller enables device support expansion through custom package upload workflows for non-Cisco devices.

Workflow

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. Add that file to Crosswork Network Controller.

What's next

Review the prerequisites for uploading custom device packages at Requirements to upload custom packages, on page 54. Then, follow the procedure to upload the custom device packages. See Upload custom packages, on page 56.

Requirements to upload custom packages

Guidelines for custom packages

You must complete these requirements when uploading custom software packages to Crosswork Network Controller:

- Upload only one file at a time. If you need to add support for a third device type, add the file to the common directory and create a replacement file containing all required files before uploading.
- Bundle all the new MIBs and the necessary dependencies to prevent import errors.
- Only upload package files with supported extensions. For collector files, the supported extensions are YANG (.yang), MIB (.mib, .my), Definition (.def), and Device Packages (.xar). For application files, the supported extensions are Device metadata (.yaml, .yml), Zips (.zip), and SDU bundle (.sdu).
- Bundle the files in the `.tar.gz` format before uploading.
- Ensure the top-level directory of the package includes at least one collector type, such as SNMP, CLI, or Common.
- Do not attempt to overwrite system MIB package files with custom MIB files; this action fails.
- When uploading an aggregate package, place files for `cli/` and `snmp/` in their respective directories and files used by both in the `common/` directory.

  Sample directory structure for an aggregate package:

```
├── 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
```

Upload considerations

When uploading custom software packages to Crosswork Network Controller, consider these:

- Updating a software package replaces the existing file.
- To upload multiple .xar files, combine them into a single .tar.gz archive before uploading.
- Do not attempt to overwrite system MIB package files with custom MIB files; this action fails.
- Ensure the .tar.gz archive contains only the package folders at the top level, without any parent or hierarchy folders.
- Crosswork Network Controller validates only the file extension and does not check the internal contents of the file.
- For validating custom MIBs and YANGs before upload, see Use Custom MIBs and Yangs on Cisco DevNet.

Performance considerations

The performance of collection jobs using custom packages depends on the optimization of those packages. Ensure that the packages are optimized for the scale of deployment before uploading them to Cisco Crosswork. For information on how to validate custom MIBs and YANGs that can be uploaded to Data Gateway , see Use Custom MIBs and Yangs on Cisco DevNet.

Third-party device considerations

When adding a custom package for third-party devices, name the sys-oids YAML file *exactly* as **third-party-sys-oids.yaml**. Use only lowercase letters for the file name and do not include any additional prefixes or suffixes. For example, do not use names like **third-party-name-sys-oids.yaml**. Place the **third-party-sys-oids.yaml** file in the `common/device-metadata/ directory` of your package.

If the file name or location is different, Crosswork Network Controller will not load the file. Ensure that you verify and update your package before uploading.

Upload custom packages

The process of adding custom packages involves bundling multiple files into a single tar.gz package format and then uploading it. This ensures that the packages are optimized and contain only the necessary files, such as supported file extensions and specific collector types, such as SNMP and CLI.

Before you begin

Confirm that you have met the prerequisites before uploading a custom package. See Requirements to upload custom packages, on page 54.

Use these steps to upload a custom software package.

Procedure

Step 1 Go to **Administration** > **Data Collectors Global Settings** > **Custom packages**.

Step 2 In the **Custom packages** page, click the add icon.

Step 3 In the **Add custom packages** window, choose the package type to import from the **Type** drop-down.

Step 4 Click the blank field in **File name** to open the file browser window.

a. Select the package you want to import.

b. 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**.

Delete a custom package

Remove custom packages that are no longer used, freeing up resources and updating collection jobs.

Deleting a custom package removes all YANG and XAR files from Cisco Crosswork and affects all collection jobs that use the package.

Procedure

Step 1 Go to **Administration** > **Data Collector(s) Global Settings> Custom packages**.

Step 2 From the **Custom packages** pane, select the package you want to delete.

Step 3 Click the delete icon.

Step 4 In the **Delete custom package** window, click **Delete** to confirm.

The custom package and its YANG and XAR files are removed, and collection jobs using the package will no longer function.

System packages

A system device package is a configuration supplied via an application-specific manifest in JSON format.

- is added or updated automatically whenever Cisco Crosswork applications are installed or updated
- enables applications to install multiple device packages as needed, and
- contains one or more separate installable file sets, with each file set in the package belonging to the same application.

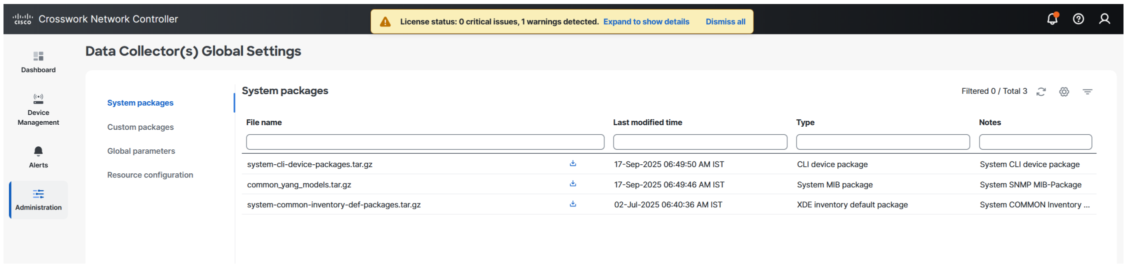
Downloading a device package

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.

1. Locate the device package you want to download in the **File name** column.
2. Click the download button next to the package name.

The device package is downloaded to your computer.

Figure 28: System device packages



Crosswork Network Controller
License status: 0 critical issues, 1 warnings detected. Expand to show details Dismiss all
Dashboard
Device Management
Alerts
Administration
Data Collector(s) Global Settings
System packages
Custom packages
Global parameters
Resource configuration
System packages
Filtered 0 / Total 3

File name	Last modified time	Type	Notes
system-cli-device-packages.tar.gz	17-Sep-2025 06:49:50 AM IST	CLI device package	System CLI device package
common_yang_models.tar.gz	17-Sep-2025 06:49:46 AM IST	System MIB package	System SNMP MIB-Package
system-common-inventory-def-packages.tar.gz	02-Jul-2025 06:40:36 AM IST	XDE inventory default package	System COMMON Inventory ...

Collection jobs in Crosswork Data Gateway

A collection job is a data collection operation that Crosswork Data Gateway executes in response to application requests. A collection job:

- enables applications to initiate data gathering from network devices
- is assigned and managed by Cisco Crosswork to a Data Gateway, and
- supports transmission using protocols such as CLI, MDT, SNMP, gNMI, and syslog.

The Data Gateway can collect any type of data as long as it is compatible with the supported protocols.

Types of collection jobs handled by Crosswork

Cisco Crosswork handles two types of data collection requests:

- Internal processes: These requests forward data for internal operations within Cisco Crosswork. Cisco Crosswork creates system jobs for this purpose.
  - If you want the Data Gateway to gather specific information from non-Cisco devices, you must use custom device packages.
  - For more information on custom device packages, see Custom Packages.
  - To learn how to build a model for Cisco Crosswork to communicate with non-Cisco devices, see Cisco DevNet.
- External data destinations: These requests forward collected data to external endpoints, such as Kafka, gRPC, or Cisco Crosswork Health Insights.
  - You can forward data to multiple destinations in a single request by adding external data destinations when creating a KPI (Key Performance Indicator) profile.
  - For more information on configuring external data destinations, see External data destinations, on page 39.
  - To learn how to create the KPI profiles, see *Create a new KPI profile* in the *Cisco Crosswork Network Controller Closed-Loop Network Automation Guide*.

Collection jobs in Crosswork Network Controller UI

On the Collection Jobs page in the Crosswork Network Controller UI, you can view active collection jobs and operational context.

The left pane on the Collection Jobs page includes two tabs:

- Bulk jobs: Lists collection jobs created by the system, UI, or API.
- Parameterized jobs: Displays active collection jobs dynamically initiated by the Crosswork Network Controller and tied to specific monitoring use cases:
  - Default jobs: Created automatically for reachability checks.
  - Policy-driven jobs: Generated when Performance Policies are applied.
  - Service-based jobs: Created as a result of enabling basic or advanced service health monitoring.

Deprecation of MDT-based data collection

Crosswork Network Controller is deprecating support for Model-Driven Telemetry (MDT) based data collection. While the MDT configuration options remain visible in the GUI for backward compatibility during the transition period, MDT collection is no longer actively supported and should not be used for new deployments.

You should migrate to gNMI for all telemetry data collection needs. The gNMI protocol provides enhanced capabilities, a richer feature set, simplified architecture, improved integration with modern network automation workflows, and ongoing support from Cisco.

Create, delete, and monitor collection jobs

In Cisco Crosswork, collection jobs describe data collection tasks that the Data Gateway performs. Use cases for creating, deleting, and monitoring collection jobs involve the following:

- Gathering device configuration, interface traffic counters, and operational metrics for network monitoring and analytics. See Create a collection job from Crosswork UI , on page 59.
- When collection jobs are no longer needed, such as outdated data requirements or device decommissioning, or when you want to clean up unused or redundant jobs after a data collection cycle is complete or after testing. See Delete collection job, on page 64.
- Verify the status of collection jobs and ensure that data is collected successfully from target devices.

Create a collection job from Crosswork UI

Configure a new collection job to gather data from network devices via the Cisco Crosswork UI.

Use this task to automate data collection from targeted network devices. You can use CLI or SNMP protocols, and the results are deposited in a specified data destination.

Before you begin

- Ensure that a data destination is created and active to deposit the collected data.
- Gather details of the sensor path and MIB that you plan to collect data from.
- Collection jobs created through the Data Gateway UI page can only be published once.
- For CLI data collection, ensure that devices do not have a banner configuration. See the device documentation on how to turn this off.

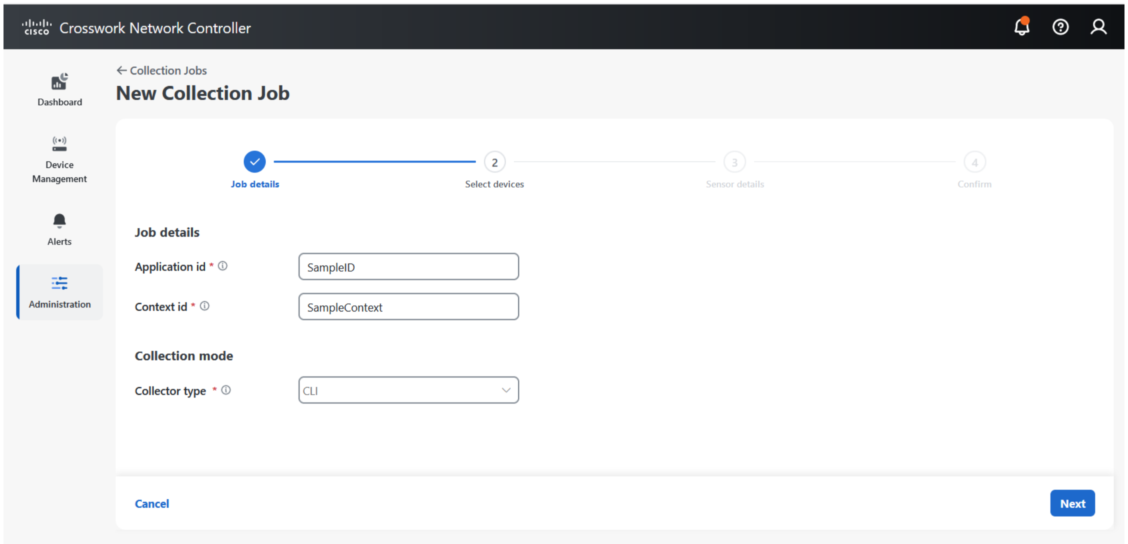
Procedure

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

Step 2 In the left pane, click +.

Step 3 On the **New Collection Job** page, enter the following:

Figure 29: New collection



New Collection Job

Job details

Application id *: SampleID

Context id *: SampleContext

Collection mode

Collector type *: CLI

a. **Application Id**: Enter a unique identifier for the application.

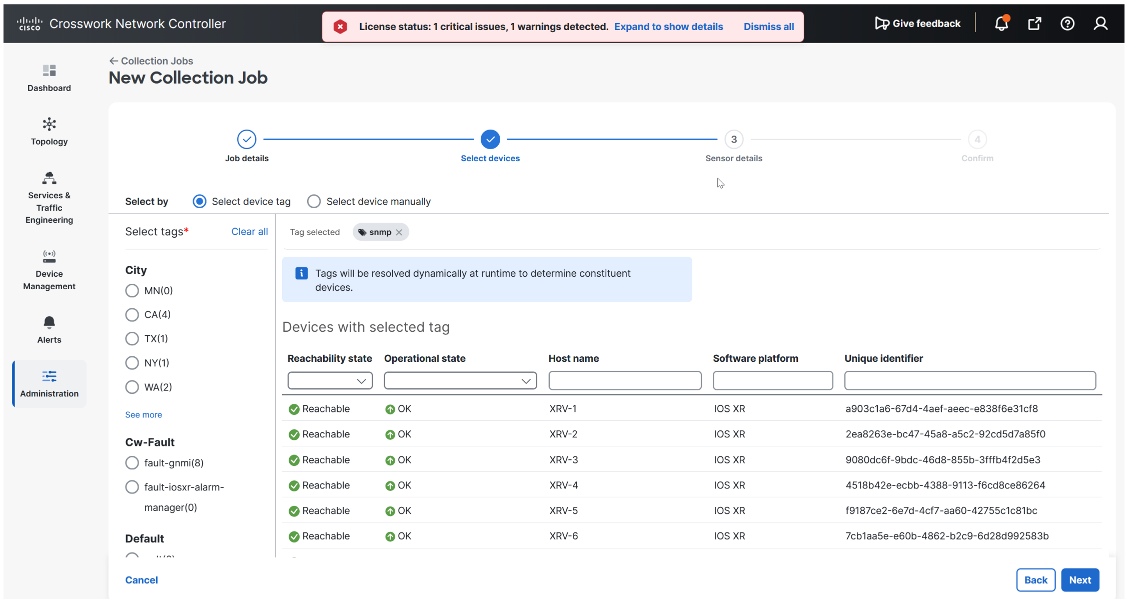
b. **Context Id**: Enter a unique identifier for your application subscription across all collection jobs.

c. **Collector type**: Select the type of collection (CLI or SNMP).

d. Click **Next**.

Step 4 Select the devices from which data is to be collected.

Figure 30: Select devices



License status: 1 critical issues, 1 warnings detected.

New Collection Job

Select by ● Select device tag ○ Select device manually

Select tags*

Tag selected: snmp

City
○ MN(0)
○ CA(4)
○ TX(1)
○ NY(1)
○ WA(2)

Cw-Fault
○ fault-gnmi(8)
○ fault-iosxr-alarm-manager(0)

Default

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

Devices with selected tag

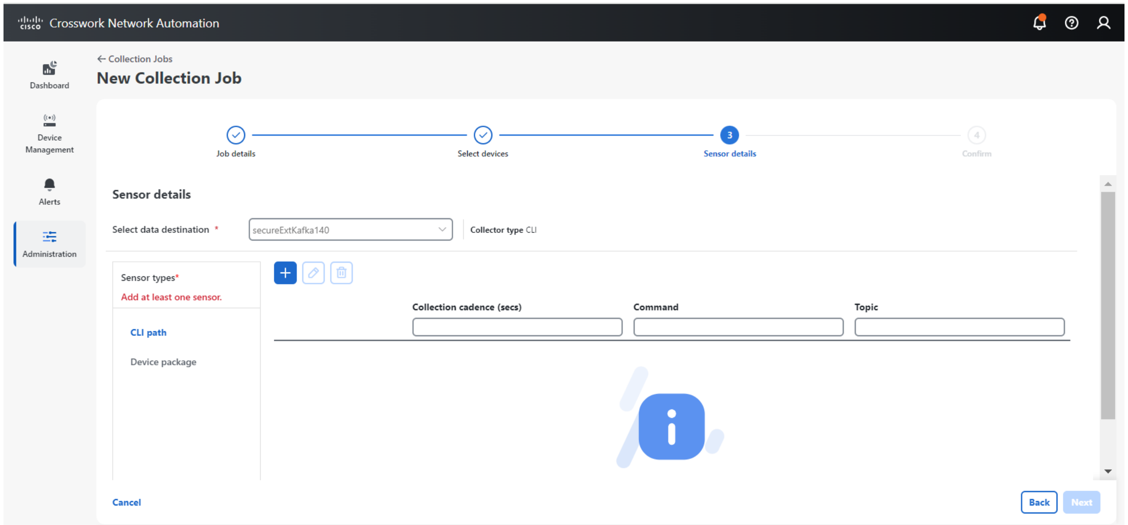
Reachability state	Operational state	Host name	Software platform	Unique identifier
Reachable	OK	XRV-1	IOS XR	a903c1a6-67d4-4aef-aeec-e838f6e31cf8
Reachable	OK	XRV-2	IOS XR	2ea8263e-bc47-45a8-a5c2-92cd5d7a85f0
Reachable	OK	XRV-3	IOS XR	9080dc6f-9bdc-46d8-855b-3fffb4f2d5e3
Reachable	OK	XRV-4	IOS XR	4518b42e-ecbb-4388-9113-f6cd8ce86264
Reachable	OK	XRV-5	IOS XR	f9187ce2-6e7d-4cf7-aa60-42755c1c81bc
Reachable	OK	XRV-6	IOS XR	7cb1aa5e-e60b-4862-b2c9-6d28d992583b

a. Select devices based on device tag or manually.

b. Click **Next**.

Step 5 Enter the sensor details. The parameters differ for CLI path, SNMP, and device package. See Parameters for configuring sensor path, on page 64.

Figure 31: Sensor details for CLI path



New Collection Job

Sensor details

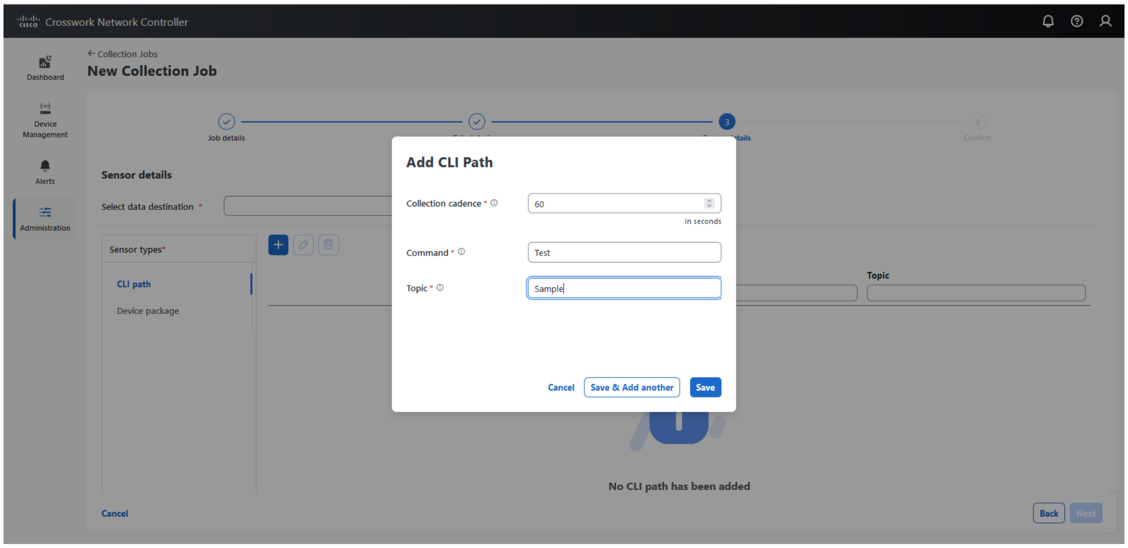
Select data destination * secureExtKafka140

Collector type CLI

Sensor types*

Add at least one sensor.

Figure 32: Add CLI path



Add CLI Path

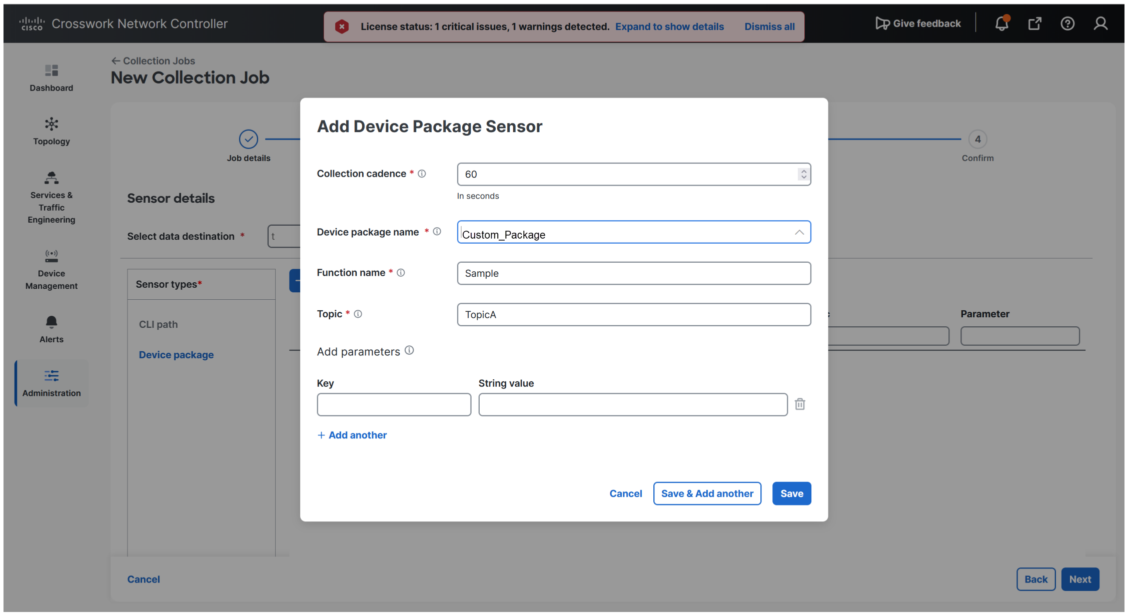
Collection cadence * 60 In seconds

Command * Test

Topic * Sample

No CLI path has been added

Figure 33: Add device package sensor



Add Device Package Sensor

Collection cadence * : 60 (In seconds)

Device package name * : Custom_Package

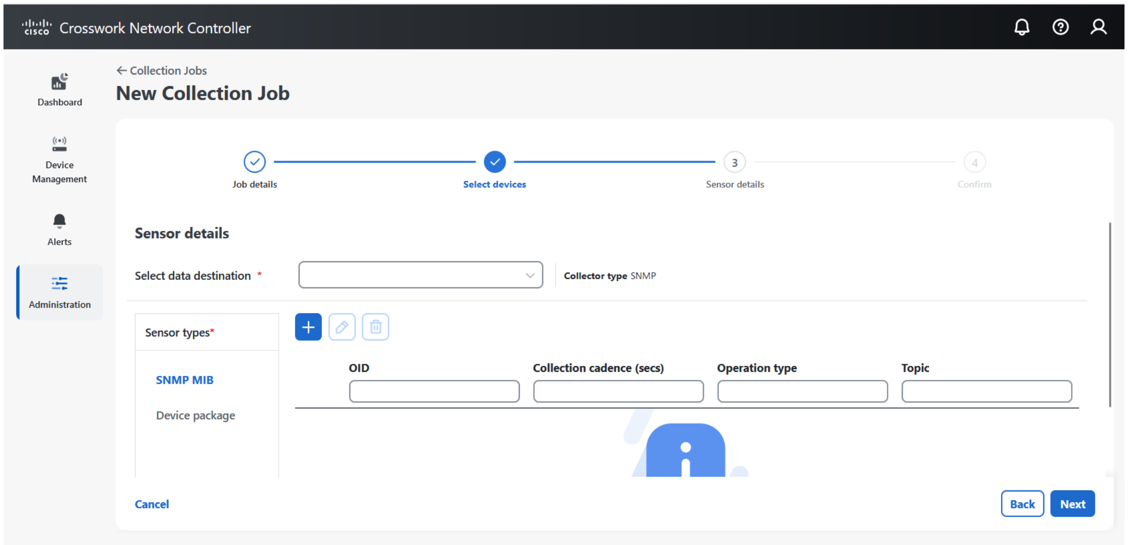
Function name * : Sample

Topic * : TopicA

Add parameters

Key	String value

Figure 34: Sensor details for SNMP path



Sensor details

Select data destination * :

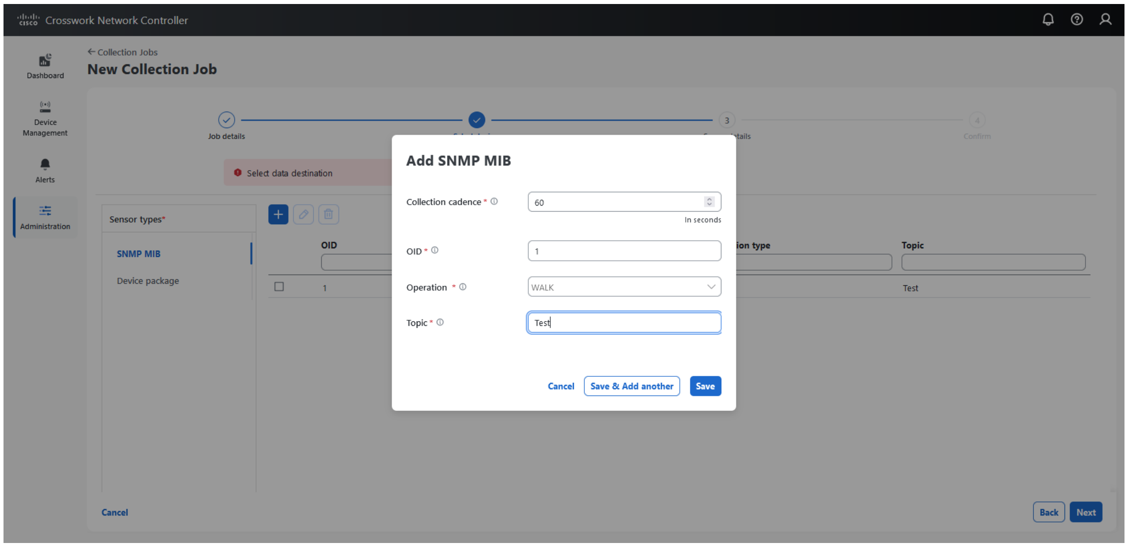
Collector type SNMP

Sensor types*

- SNMP MIB
- Device package

OID	Collection cadence (secs)	Operation type	Topic

Figure 35: Add SNMP MIB



New Collection Job

Select data destination

Sensor types*
SNMP MIB
Device package

	OID	…ion type	Topic
□	1		Test

Add SNMP MIB

Collection cadence * ⓘ: 60 (In seconds)
OID * ⓘ: 1
Operation * ⓘ: WALK
Topic * ⓘ: Test

Cancel | Save & Add another | Save

Step 6 Click **Create Collection Job**.

Note

If you submit a collection job to an external Kafka destination using unsecured Kafka, the dispatch to Kafka will fail to connect. Collector logs will show a timeout exception, and Kafka logs will display an SSL authentication error. This issue occurs because the port on the external Kafka VM is blocked. 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. To check if the port is listening on Kafka docker/server port, use `netstat -tulpn`.

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

Recommendations for data collection

Best practice for setting data collection cadence

When configuring data collection cadence:

- Set the cadence to a minimum of 60 milliseconds.The valid range for configuring cadence is between 10 milliseconds and 604,800,000 milliseconds.
- Consider both the frequency with which device data changes and the operational significance of that data.
- Use a longer intervals (higher cadence) for relatively stable information, such as memory consumption or CPU utilization.
- Use a shorter cadence for more volatile or dynamic data points.

- If a Data Gateway is set to collect large volumes of telemetry or extensive datasets with a short cadence, this will increase the load on both the devices and the Crosswork Network Controller. Because it is challenging to model these loads precisely, experiment to identify settings that provide the best operational insight and, most importantly, actionable information.

Handling skipped collection attempts

If a collection attempt is skipped because the previous execution is ongoing, Crosswork Data Gateway logs a warning without an alert. This avoids overlapping collection jobs while maintaining operational efficiency.

Parameters for configuring sensor path

This section describes the parameters that you must provide for configuring the sensor paths.

Table 7: Sensor details required for adding the CLI and SNMP collection

Parameter	Description
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 XDE device package.
Operation	Select the operation from the list.
OID	Specifies the SNMP Object Identifier used in sensor paths for polling specific metrics from network devices.
Command	CLI command
Topic	Topic associated with the output destination. Topic can be any string if using an external gRPC server.

Delete 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:

Procedure

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.

Monitor the collection jobs

Monitor the status of active collection jobs on Crosswork Data Gateway instances enrolled with Crosswork Network Controller by using the Collection Jobs page.

Before you begin

When monitoring collection jobs, be aware of these important status behaviors and conditions that affect task visibility and job health:

- The status of a collection task is initially reported as Unknown after a device attaches to a Crosswork Data Gateway due to pending data collection or reporting delays.
- Reasons for Unknown status include
  - unreported status by the Data Gateway
  - loss of connection between Data Gateway and Crosswork,
  - pending telemetry collection, such as traps not being sent to the Data Gateway southbound interface or the device not sending telemetry updates.
  - lack of triggered SNMP trap conditions. 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.
- Collection jobs change to Successful when data is processed without errors, or Failed otherwise.
- A degraded collection job may indicate missing static routes to the device or misconfigured KPI job mappings to standard instead of extended Data Gateway instances.
- Data collections continue even if a destination is in an Error state, but error counts increment and require log review and troubleshooting.
- Address NSO-related job creation failures by resolving NSO errors and resetting device administrative states to restart collection properly.

Use these steps to view and understand the collection job details.

Procedure

Step 1 From the main menu, 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 remove collection jobs. You can also refresh the status of a collection job and its associated tasks.

Step 2 Select a job in the **Collection Jobs** pane.

The **Job Details** pane displays the application name and context associated with the collection job, status of the collection job, and other job-related details.

Job details pane

Selecting a job displays detailed information on all collection tasks associated with that job. The details are:

- The Application name and context associated with the collection job.
- The collection job status.
- The device hostname and unique device ID.
- The sensor data paths and destination information are displayed.
- Job configuration of the collection job that you pass in the REST API request. To view the job configuration, Click ⓘ icon next to **Config Details**. Data Gateway lets you view configuration in two modes:
  - View Mode
  - Text Mode
- The collection type is displayed.
- The time and date when the collection job was last modified.
- 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. (y) Issues is the count of output collections in UNKNOWN or FAILED state.

Data Gateway also displays these details for collections and distributions:

Field	Description
Collection/Distribution Status	Split into multiple cells if describing a process and providing an instruction, otherwise clarify the instructions and context. Click ⓘ next to the collection/distribution status for details.
Hostname	Device hostname with which the collection job is associated.
Device Id	A unique identifier for the device from which data is collected.

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

Collection job status explanations and error handling

Event-based collection jobs

The status of event-based collection jobs in Crosswork Data Gateway reflects the current data collection state and device connectivity with the system.

- When data collection completes successfully, the collection job status changes from **Unknown** to **Success** in the **Collection Jobs** pane.
- When a device is detached from the Crosswork Data Gateway, all associated collection jobs are automatically deleted. The job status displays as **Success** in the **Collection Jobs** pane, but no devices or collection tasks appear in the **Job Details** pane.
- When a device is newly attached to a Crosswork Data Gateway, a new collection job is created with the initial status **Unknown**. The status automatically updates to **Success** once event data is received from the device.

- If a device configuration is modified incorrectly after it has already been attached and the Crosswork Data Gateway has received both the job and event data, the collection task status remains unchanged in the **Job Details** pane.
- If the device inventory is updated with an incorrect device IP address, the collection task status is displayed as Unknown in the **Job Details** pane.

Handling errors and failures

A Create Failed error indicates that one or more devices failed to complete the setup process out of the total number of devices (N). Data collection continues for the devices that were successfully set up.

You can identify the devices causing the setup failure using the Control Status API.

- Resolving NSO errors: If job creation fails on a device due to NSO (Network Services Orchestrator) errors, follow these steps after fixing the NSO configuration:
  1. Manually change the device’s administrative state to Down.
  2. Change it back to Up.

Note This action resets the data collection process on the device.

- Viewing and resolving other job errors
  - Errors that occur during job creation or deletion are displayed in a separate pop-up window.

    To view the details, click the information icon next to the job status.
  - If necessary, recreate the job by sending a PUT Collection Job API request with the identical payload.

CLI collection jobs

CLI Collection Jobs are a method supported by Crosswork Data Gateway to collect CLI-based data from network devices. These jobs use specific commands to retrieve operational data. They diagnose network issues and gather directory information from the device. The commands supported include:

- show (and its short version `sh`)
- `traceroute`
- `dir`

CLI collection API payload example

This section provides a sample payload for the CLI Collection API, illustrating its structure and key elements.

In this example, Crosswork sends device data to an external Kafka destination. The Device Lifecycle Manager assigns a UUID for identification. This UUID uniquely identifies each device. The device is identified with a UUID rather than an IP address. The destination is also referenced by a UUID. Cisco Crosswork looks up the UUIDs for collection jobs built using the UI. If you create your own collection jobs, you must look up these values yourself.

```
{
  "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"
        }
      }
    ]
  }
}
```

Steps to create a CLI collection job

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

SNMP collection jobs

An SNMP collection job is a task configured on the Cisco Crosswork Data Gateway that directs the system to collect device data using SNMP protocol. It is a type of collection job that:

- Polls devices based on their supported MIB and associated Object Identifiers (OIDs) to retrieve specific data
- Can be configured to collect multiple types of SNMP data, such as scalar values or tables, across multiple devices, and

- Executes the collection requests and stores or forwards the retrieved data to designated external data destinations for further processing or analysis.

SNMP collection methods

You can configure SNMP data collection in two primary ways:

- MIB-based polling: Data is collected based on MIB and OID definitions supported by the device through polling operations.
- Trap-based listening: The collector listens for incoming SNMP traps to collect event-driven data.

SNMP polling and trap-based listening

Many common device attributes can be collected using standard MIBs, which are included with Cisco Crosswork. However, if a device uses custom or vendor-specific MIBs, you may need to upload a custom MIB package tailored for that device. For information about the packages, see Types of custom packages, on page 53.

Crosswork Data Gateway supports these SNMP versions for polling and traps:

Table 8: Supported SNMP versions

Purpose	Supported versions
Polling data	• SNMPv2 • SNMPv3 (no auth nopriv, auth no priv, authpriv) • Supported auth protocols: HMAC_MD5, HMAC_SHA, HMAC_SHA2-512, HMAC_SHA2_384, HMAC_SHA2_256, and HMAC_SHA2_224 • 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)

Device configuration sample commands

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

Table 9: Sample configuration to enable SNMP on a 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.

Note

- SNMPv3 user passwords must be at least 8 bytes.
- The IP address in trap commands should be the virtual IP address of the Crosswork Data Gateway.

SNMP collection job operations

The SNMP Collector supports several SNMP operations defined in the sensor configuration:

- SCALAR: Retrieves single data points. Multiple scalar OIDs can be retrieved efficiently using a single GETBULK (`getbulkrequestquery`) request.

- TABLE, WALK, COLUMN: Retrieve tabular and structured data as specified. For TABLE operation, either provide a Table OID or a Column OID.

Note The optional device parameter `snmpRequestTimeoutMillis` should be set if the device's response time exceeds 1500 milliseconds. Use it only when you are sure the device responds slowly. Specify the value in milliseconds, with a default and minimum of 1500 ms. There is no maximum limit for this value.

SNMP collection job example

```
{
  "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"
    }
   }
  ]
 }
}
```

Steps to create a SNMP collection job

You can create a SNMP collection job using the Cisco Crosswork UI or APIs. For information on creating a job from the UI, see Create a collection job from Crosswork UI , on page 59 and from the API, see Cisco Devnet.

SNMP traps collection job

SNMP trap collection jobs can only be created through the API.

Prerequisites for trap collections

- Install the Common EMS Services application.
- Configure host information for SNMP on the Data Gateway.
- Ensure SNMP traps are properly configured on devices to send traps to the Crosswork Data Gateway's virtual IP address.

To understand how SNMP trap collection operates, see How SNMP trap collection jobs work, on page 77.

Supported trap types

Crosswork supports three types of non-YANG or OID-based traps:

Table 10: Non-YANG and OID traps

Sensor path	Description
*	Gets all the traps pushed from the device without any filter.

Sensor path	Description
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)

Enabling SNMP traps to forward to external applications

We recommend enabling only the necessary traps on the device. You can identify trap types in the received data by matching OIDs (OBJECT_IDENTIFIER), for example *oid* `1.3.6.1.6.3.1.1.4.1.0` and *strValue* associated to the *oid* in the OidRecords. The application matches the OID of interest to determine the trap type.

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

Table 11: Non-YANG and OID traps

Trap type	OID value
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`

Example to forwards the SNMP traps to an external applications

```
{
  "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"
    }
  ]
}
```

Example SNMP trap payload for external applications

A sample payload illustrates trap forwarding with relevant OID records and their corresponding string values.

```
{
  "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"
        }
      }
    ]
  }
}
```

How SNMP trap collection jobs work

SNMP trap collection jobs can only be created through the API. Trap listeners in the Data Gateway listen on UDP port 1062 for trap data. They forward the data based on configured recipient topics.

Summary

Key components involved in the SNMP trap collection job process:

- Data Gateway: The component that receives SNMP trap messages and forwards relevant data based on active collection jobs and configured recipient topics.
- Trap listener: The sub-component within the Data Gateway that listens for incoming SNMP traps on UDP port 1062.
- Recipient topic: The configuration element that determines where the Data Gateway forwards validated SNMP trap data.
- Device or router: The network element that generates and sends SNMP traps to the Data Gateway.

Workflow

When an SNMP trap is received, the Data Gateway:

1. Checks for an active collection job for the device.
2. Validates the trap version and community string.

Note To prevent Data Gateway from checking the community string for SNMP traps, select the **SNMP Disable Trap Check** check box when adding a device through the Crosswork UI. For more information about this option, see *Add devices through the UI* in the *Cisco Crosswork Network Controller 7.1 Device Lifecycle Management*.

3. For SNMP v3, the process validates user authentication, privacy protocols, and credentials.

Note SNMPV3 auth-priv traps depend on the engineId of the device or router to maintain local USM user tables. If the engineId of the device or router changes, receiving traps will be interrupted. Therefore, there will be an interruption in receiving traps whenever the engineId of the device or router changes. To resume receiving traps, detach and reattach the respective device.

4. Filters the traps based on the trap OID mentioned in the sensor path and sends only those requested.

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

MDT collection job

Model-Driven Telemetry Collection in Crosswork Data Gateway is a network data collection method that

- enables direct consumption of telemetry streams from IOS-XR devices using MDT TCP Dial-out mode
- leverages Cisco NSO to automate telemetry configuration and collection job deployment, and
- requires backup or restore operations to be coordinated with NSO for device configuration consistency.

Important Starting with Crosswork Network Controller Release 7.2, Model-Driven Telemetry (MDT) based data collection is deprecated. While MDT options remain visible in the GUI during this transition period, use gNMI for all new and existing telemetry collection configurations. See Deprecation of MDT-based data collection, on page 59.

Notes on backup and restore

- If MDT collection jobs are changed between backup and restore operations, Crosswork Network Controller only restores jobs in the database and does not replay configuration updates on the devices. NSO or device configuration restoration is required separately.
- Before using any YANG modules for MDT collection, verify their support status. See List of Pre-loaded YANG Modules for MDT Collection.

Example 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"
  }
 }
}
```

How does MDT collection work

Summary

The MDT collection job workflow orchestrates automated telemetry data collection from network devices, ensuring that key performance indicators (KPIs) are monitored efficiently. It coordinates interactions between Cisco Crosswork, NSO, and Crosswork Data Gateway to push device configurations, create collection jobs, and distribute collected data to designated destinations.

Workflow

The MDT collection job workflow proceeds through these stages:

1. When an MDT-based KPI is activated on a device, Cisco Crosswork sends a configuration request to NSO to enable data collection on the target devices.
2. A collection job create request is sent to the Crosswork Data Gateway.
3. Crosswork Data Gateway creates a distribution to send the collected data to the specified destination.

Syslog collection jobs

A syslog collection job is a task configured on the Cisco Crosswork Data Gateway that

- collects syslog messages from devices formatted according to supported standards (RFC 5424 and RFC 3164),
- supports multiple syslog transport methods, enabling collection of real-time event logs across diverse devices, and
- processes and forwards the collected syslog data to specified external destinations for monitoring, analysis, and troubleshooting.

Filtering the syslog events

You can manage and control the volume of syslog data collected from devices by configuring filtering rules using SyslogSensors. SyslogSensors support PRI-based and filter-based rules that allow you to selectively capture only the syslog events relevant to your network monitoring and analysis needs. When you apply filters based on severity, facility, or regular expressions, only required events are forwarded to the configured destination. This reduces noise, optimizes storage, and streamlines downstream processing of syslog data. Logical operators such as AND and OR enable you to define up to three filter combinations, providing flexibility in how filters are evaluated.

Configure syslog data collection from Crosswork Data Gateway

Use the Data Gateways in your network to enable syslog data collection. This process allows you to gather and manage system logs from connected devices efficiently

Procedure

Step 1 Install the Element Management Functions application. Then, configure the host information for syslog. See the *Cisco Crosswork Network Controller 7.2 Installation Guide* for reference.

Step 2 Add the device and select the `YANG_CLI` capability.

Step 3 Configure the required parameters to enable syslog data collection from the Data Gateways.

Note
The order of these steps does not affect the outcome, but steps 2 and 3 are mandatory. If either step is skipped, no syslog data will be collected.

What to do next

For example configurations, refer to:

- Syslog collection job output, on page 81.
- Sample syslog collection payload, on page 84.
- Refer to your platform-specific documentation for additional configuration guidelines.

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.

1. Output for UNKNOWN syslog format: 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. Output for RFC5424 syslog format: 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 the device (RAW) and the RFC5424 best-effort parsed syslog events from the device.

Note The syslog collector will parse the syslog event on best effort 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>(-|\\[.+\\]))\
<message>.+)$";
```

Sample output:

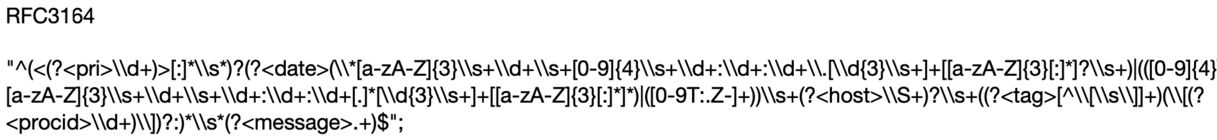
```
....
....


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. Output for RFC3164 syslog format: If the device is configured to generate syslog events in RFC3164 format and the RFC3164 format is selected in the Syslog Format field, the Syslog Job Collection output contains both RAW (as received from the 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 this 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+)|(([0-9]{4}
[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
}
....
....
```

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"
  }
 }
}
```

Configuring syslog on devices

Enable network devices to send event logs and messages to Crosswork Data Gateway for centralized monitoring and analysis by configuring non-secure or secure syslog options.

Syslog in Crosswork Data Gateway enables network devices to send logs and event messages to the Data Gateway. This allows centralized monitoring and analysis. There are two primary configurations:

- Non-secure syslog sends messages from devices to the Crosswork Data Gateway using standard, unencrypted protocols such as UDP or TCP. See Configure non-secure syslog on a device, on page 90.
- Secure syslog improves message integrity and confidentiality by using encrypted communication channels such as TLS. See Configure secure syslog on device, on page 85.

Configure secure syslog on device

In a dual-stack Crosswork deployment, the device must use the same IP stack (either IPv4 or IPv6) as configured in the device inventory to ensure syslog events are logged without interruption. If the Data Gateway host address resolves to both IPv4 and IPv6, configure the device so that the source IP in events matches the configuration in the device inventory.

Before you begin

Confirm device inventory and Data Gateway configurations use the correct IP stack.

Before you begin

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

Procedure

Step 1 Download the Cisco Crosswork trust chain.

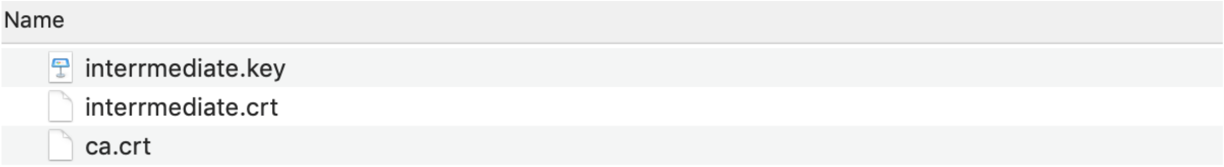
a. Access the Cisco Crosswork UI.

b. Go to **Administration** > **Certificate Management**.

c. Locate Crosswork-Device-Syslog and click the info icon.

d. Click Export All to download the certificate files to your system.

The following files are downloaded to your system.



Name
interrmediate.key
interrmediate.crt
ca.crt

Step 2 Configure your device with the Cisco Crosswork trustchain. Refer to sample configurations for device OS. Refer to the sample configurations to enable Cisco Crosswork Trustpoint on device.

a. For Cisco IOS XR.

Enable TLS and create syslog-root trustpoint:

```
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#
```

b. Enable TLS on IOS XE device configuration.

```
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
```

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

1. 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>
   ```

2. 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
   ```

Your device is configured for secure syslog communications using TLS, with trusted certificate enrollment. Syslog events will log without interruption according to inventory IP stack and FQDN configuration.

What to do next

Monitor syslog event flow on Cisco Crosswork to validate successful and secure logging from your device.

Configure non-secure syslog on a device

Configure the device to send non-secure syslog messages in RFC3164 or RFC5424 format to the Data Gateway host.

In dual-stack Crosswork deployments, ensure devices use the same IP stack (IPv4 or IPv6) for sending syslog events as configured in device inventory. Set the Data Gateway host as an IP address rather than an FQDN to ensure source IP consistency.

Before you begin

- Verify syslog configuration supports RFC3164 or RFC5424 formats.
- Ensure the device's syslog format matches the format specified during onboarding in the Crosswork UI.
- In dual-stack deployments, configure the device to send syslog over the same IP stack (IPv4 or IPv6) as in device inventory.
- Use an IP address for the Data Gateway host instead of an FQDN to ensure source IP consistency.

Procedure

Step 1 Configure syslog for RFC3164 format.

- On IOS XR, apply:

```
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>
```

- On IOS XE, apply:

```
no logging message-counter syslog
logging trap <severity>
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
```

Step 2 Configure syslog for RFC5424 format.

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

- On IOS XR, apply:

```
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
```

- On IOS XE, apply:

```
no logging message-counter syslog
logging trap <severity>
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
```

The device sends non-secure syslog messages to the Data Gateway host using the designated format and protocol.

What to do next

Verify that syslog events are being successfully received by the Data Gateway.

gNMI collection jobs

A gNMI collection job is a telemetry data collection process that

- uses the gRPC Network Management Interface (gNMI) Dial-In protocol to stream telemetry data based on defined subscriptions
- relays subscription responses (notifications) to configured destinations with preference for secure connections, and
- automatically re-subscribes existing subscriptions after device reloads while operating within the protocol’s limitations (no destination or dispatch cadence support).

Modes supported in secure and insecure GNMI collection

In gNMI, a device can operate in both secure and insecure modes simultaneously. The Crosswork Network Controller preferentially uses secure mode, depending on inventory information. After a device reloads, the gNMI collector re-subscribes the existing subscriptions to the device.

Crosswork Data Gateway supports these subscribe options for gNMI:

Table 12: gNMI subscription options

Type	Subtype	Description
Once	None	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	The router or device chooses the mode of subscription on a per-leaf basis depending on the subscribed path, such as SAMPLE or ON_CHANGE.

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 Protocol Buffers (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;
  }
  ```

Example of gNMI collection payload

In this sample you see two collections for the device group "milpitas". The first collection job gathers interface statistics every 60 seconds using the "SAMPLE" mode. The second job detects any changes to the interface state (up or down) and sends them to the collector using the "STREAM" mode.

```
{
    "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 Data Gateway

Enable secure gNMI communication between network devices and Cisco Crosswork Data Gateway by configuring trusted certificate authority settings and required device protocols. This ensures all gNMI connections are authenticated and encrypted, allowing Crosswork to safely collect and manage telemetry data from supported devices.

Cisco Crosswork supports only one root CA certificate (either self-signed or signed by a trusted root CA), which means all device certificates must be signed by the same CA. If your device certificates are signed by a different trusted root CA, you can skip the first step and start by importing the root CA certificate into Cisco Crosswork.

Procedure

Step 1 Generate certificates: Create certificates using OpenSSL or a compatible utility. For device certificates, you can include multiple device IPs in the certificate's subject alternative name (SAN). The certificate validity period should be set appropriately (recommendation: 365 days). See Generate device certificates, on page 95.

Step 2 Upload the Root CA Certificate to Crosswork: Use the Cisco Crosswork UI under **Administration** > **Certificate Management** to upload the root CA certificate. Multiple device trust chains can be combined into a single .pem file for upload. See Add the gNMI certificate, on page 96.

Note
If the gNMI certificate is already configured, update the existing .pem file to include any new trust chain information.

Step 3 Import and install certificates on devices.

- Cisco IOS XR Devices: Copy `rootCA.pem`, `device.key`, and `device.crt` to the device (usually to `/tmp`), then place them under `/misc/config/grpc` as `ca.cert`, `ems.key`, and `ems.pem` respectively. Restart TLS on the device by toggling the TLS setting.
- Cisco IOS XE Devices: Use the CLI `crypto pki import` commands to import CA certificates, device keys, and device certificates under a trustpoint. Disable revocation check if needed.

Step 4 Update device protocol configuration from Crosswork: After uploading certificates, update device settings with the secure gNMI port (GNMI_SECURE) either via Cisco Crosswork UI (**Device Management > Network Devices**) or by importing a CSV file with protocol details. See Update device protocol.

Step 5 Configure device for gNMI.

- Cisco IOS XR: Enable gRPC over HTTP/2, configure the gRPC port (range 57344–57999), and set session parameters such as TLS, trustpoints, and stream limits.
- Cisco IOS XE: Enable gNMI in insecure or secure mode with trustpoints and secure ports via CLI commands.

See Configure device for gNMI, on page 100.

Step 6 Enable gNMI bundling on IOS XR devices: gNMI bundling stitches multiple update messages into a single notification to optimize telemetry data. This feature is supported on IOS XR release 7.81 and later. See Configure gNMI bundling for IOS XR, on page 102.

Generate device certificates

Use this task to generate device certificates using OpenSSL or Microsoft utilities. These certificates are required for secure device communication and authentication.

This procedure describes the steps to create device certificates with OpenSSL. If you want to use a utility other than OpenSSL or Microsoft, contact the Cisco Support Team for guidance.

Before you begin

Use these steps to generate certificates validated with Open SSL and Microsoft utilities.

Procedure

Step 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 this command, the `days` attribute determines the how long the certificate is valid. The minimum value is 30 days, so you must update the certificates every 30 days.

Step 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, you can specify several device IP addresses separated by commas in `subjectAltName` instead of creating multiple device certificates.

```
# openssl x509 -req -extfile <(printf "subjectAltName=IP.0: 10.58.56.18, IP.1: 10.58.56.19, IP.2:
10.58.56.20 .....
```

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

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

Sample certificate 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
```

Add the gNMI certificate

Crosswork Data Gateway is the gNMI client, and the device is the gNMI server. To validate the device, Crosswork Data Gateway uses a trust chain.

Note You can upload only one gNMI certificate to Crosswork.

To add the gNMI certificate.

Before you begin

You should have a global trust chain for all devices.

Procedure

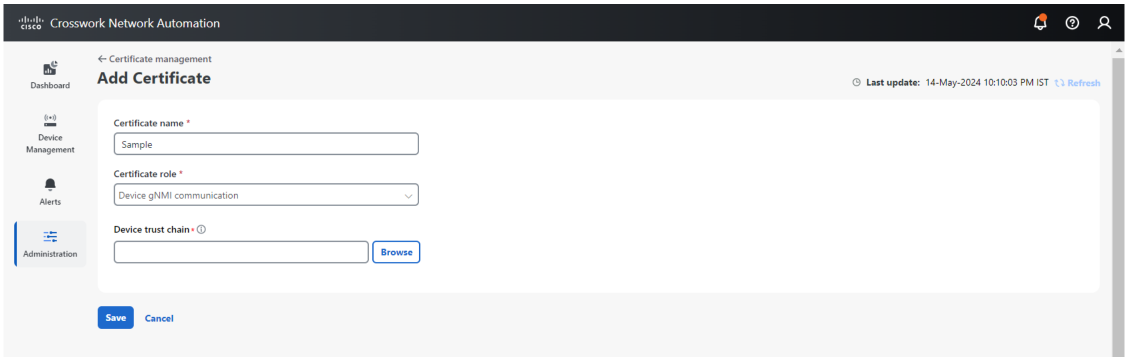
Step 1 From the Cisco Crosswork UI, go to **Administration** > **Certificate Management**.

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/gRPC communication" from the drop-down list.
- **Device trust chain**: Browse your local file system to the location of the rootCA file and upload it. 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.

Figure 36: Add certificate



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

Certificate name *: Sample

Certificate role *: Device gNMI communication

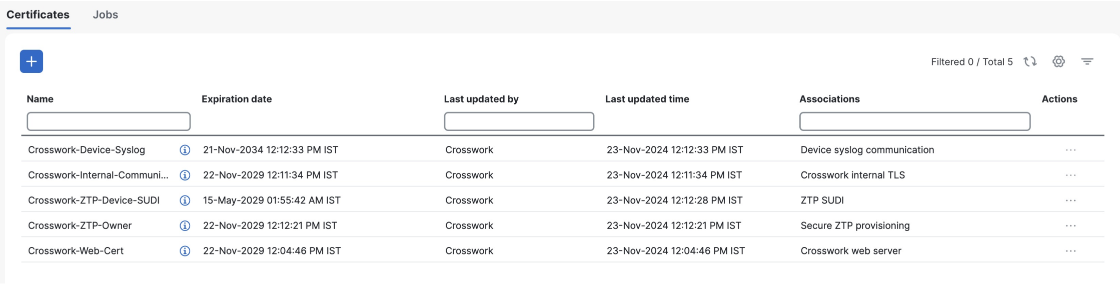
Device trust chain *

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**.

After you add the gNMI certificate, it appears in the configured certificates list.

Figure 37: Certificates management



Name	Expiration date	Last updated by	Last updated time	Associations	Actions
Crosswork-Device-Syslog ⓘ	21-Nov-2034 12:12:33 PM IST	Crosswork	23-Nov-2024 12:12:33 PM IST	Device syslog communication	···
Crosswork-Internal-Communi... ⓘ	22-Nov-2029 12:11:34 PM IST	Crosswork	23-Nov-2024 12:11:34 PM IST	Crosswork internal TLS	···
Crosswork-ZTP-Device-SUDI ⓘ	15-May-2029 01:55:42 AM IST	Crosswork	23-Nov-2024 12:12:28 PM IST	ZTP SUDI	···
Crosswork-ZTP-Owner ⓘ	22-Nov-2029 12:12:21 PM IST	Crosswork	23-Nov-2024 12:12:21 PM IST	Secure ZTP provisioning	···
Crosswork-Web-Cert ⓘ	22-Nov-2029 12:04:46 PM IST	Crosswork	23-Nov-2024 12:04:46 PM IST	Crosswork web server	···

Import and install certificates on devices

Import and install certificates on the IOS XR and XE devices. Certificates and trustpoints are required only for secure gNMI servers.

Procedure

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

Step 2 Log in to the IOS XR device and enter the VM shell.

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

Step 3 Navigate to the directory.

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

Step 4 Create or replace the content of these files.

Note
If TLS was previously enabled on your device, these files will already be present. In this case, replace the content of these files as explained in this section. 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

Step 5 Restart TLS on the device to apply the changes. To do this, disable TLS by using the "no-tls" command and then re-enable it by entering the "no no-tls" configuration command.

Example 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 Crosswork

Perform the update of protocol details for a specified device using the Crosswork Network Controller.

Use this task to establish or update device communication security, particularly after certificate configuration or when maintaining compliance with network security protocols.

Before you begin

- Ensure you have configured the gNMI certificate in Crosswork Network Controller.
- Prepare the CSV file containing device details, including the required protocol information.

Procedure

Step 1 After configuring the gNMI certificate in Crosswork Network Controller, ensure your device is listed in the network inventory.

Step 2 Update the device with secure protocol details:

a) Use the Cisco Crosswork UI at **Device Management > Network Devices**.

b) Specify protocol details as GNMI_SECURE Port in the CSV file corresponding to the device.

c) Import the device entry or edit it if necessary.

d) View the **Edit Device** page for confirmation.

The device is updated with the specified secure protocol settings, and the Crosswork inventory should reflect the new configurations.

What to do next

- Validate device communication and ensure connectivity using updated protocols.
- Monitor alerts and error messages related to protocol changes.

Configure device for gNMI

Configure your device for gNMI support to enable remote management and programmability using standardized network management protocols.

The gNMI protocol enables centralized and automated management of network devices.

Procedure

Step 1 Enable gRPC over an HTTP/2 connection.

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

Port numbers range from 57344 to 57999. If the specified port number is unavailable, the system displays an error message.

Step 2 Configure 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 }
```

Table 13: Parameters for gNMI session configuration

Parameters	Description
address-family	Configure the address family identifier type.
dscp	Configure the QoS marking DSCP on transmitted gRPC.

Parameters	Description
max-request-per-user	Configure the maximum concurrent requests per user.
max-request-total	Configure the maximum concurrent requests in total.
max-streams	Configure the maximum number of concurrent gRPC requests. The maximum subscription limit is 128 requests. The default is 32 requests.
max-streams-per-user	Configure 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 a trustpoint.
server-vrf	Enable the server VRF.

Step 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
```

Configurations for Cisco IOS XE devices

This 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 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
```

Configure gNMI bundling for IOS XR

In IOS XR, gNMI bundling collects multiple Update messages within the Notification message of a SubscribeResponse. These messages are delivered to the IOS XR device. To use gNMI bundling, you must enable it and set the message size.

Before you begin

Be aware of these points:

- 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.

Procedure

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 smaller than the bundling size, the system may add another instance. This can cause the total size to exceed the bundling limit.

What to do next

Verify that the bundling capability is configured using the configuration.

```
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)
```

Troubleshooting options and common issues in Crosswork Data Gateway

This section provides information about the troubleshooting options available in Crosswork Data Gateway and outlines common issues that may arise, along with guidance on diagnosing and resolving them.

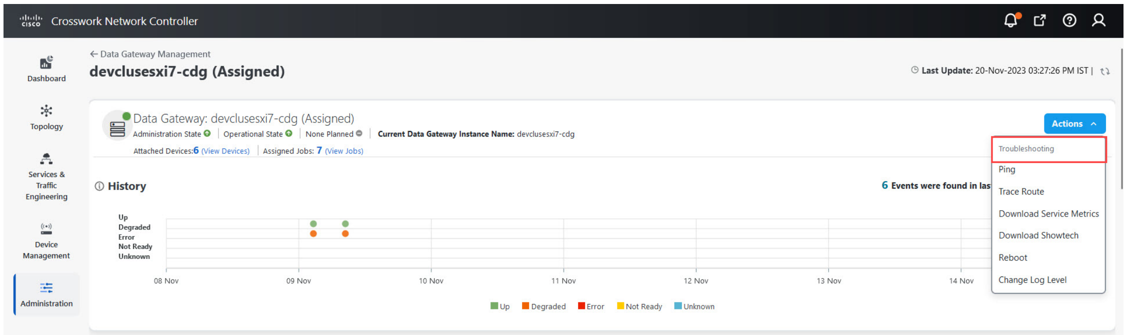
Use this section to access topics related to troubleshooting options and common issues in Crosswork Data Gateway.

- Use the troubleshooting options available in the Crosswork Network Controller UI to diagnose and resolve issues with Crosswork Data Gateway instances. See Troubleshooting actions available from Crosswork, on page 103.
- Use these procedures to quickly identify and resolve operational disruptions, restore service continuity, and maintain reliable data collection performance. See Troubleshooting common issues, on page 108.

Troubleshooting actions available from Crosswork

This section provides information about the troubleshooting options available in Crosswork Data Gateway through the Crosswork Network Controller UI.

Figure 38: Troubleshooting actions



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

Use these actions from the Data Gateway details page to diagnose and resolve issues:

- Check Data Gateway connectivity, on page 103
- Download service metrics, on page 33
- Download the showtech logs, on page 105
- Reboot Data Gateway VM, on page 34
- Change the log level of components , on page 107

Check Data Gateway connectivity

Verify that you can reach a target destination from a Data Gateway to ensure that network connectivity is available for troubleshooting or validation.

Use the Ping and Traceroute actions provided within the Crosswork Data Gateway Management interface to check connectivity to network destinations.

Before you begin

Enable ping traffic on the network to allow successful ping requests.

Use these steps to check Data Gateway connectivity.

Procedure

Step 1 Go to **Administration** > **Data Gateway Management** > **Data gateways** in the Crosswork interface

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

Step 3 On the **Data Gateway details** page, at the top right corner, click **Actions** and choose one of the options.

- **Ping**: Enter values for number of packets and destination address, then click **Ping**.
- **Traceroute**: Enter the destination address and click **Traceroute**.

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

The destination's reachability status and details of the Ping or Traceroute test are displayed, confirming network connectivity.

Download service metrics

Download and decrypt service metrics for data gateway instances from the Crosswork UI.

Use this procedure to retrieve encrypted metrics files for all collection jobs from a Data Gateway for analysis or troubleshooting.

Before you begin

Ensure that you meet these requirements during decryption:

- Use OpenSSL version 1.1.1i or newer. To check, use `openssl version`.
- On a Mac, ensure that you are not using LibreSSL, as it does not support the necessary switches.
- The metrics file must have a `.tar.xz` extension.

Procedure

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 **Data Gateway details** page, on the top-right corner, click **Actions** > **Download Service Metrics**.

Step 4 Enter a passphrase.

Note
Make a note of this passphrase because you will use it later to decrypt the file.

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

Step 6 After the download, decrypt the file using the OpenSSL command.

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<password>
```

Example:

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in show-tech-file.tar.xz.enc -out
show-tech-file.tar.xz -pass pass: myPassword
```

- Do not enclose filenames in quotation marks when running the command.
- Use OpenSSL version 1.1.1i to decrypt the file. To check the OpenSSL version on your system, use the command `openssl version`.
- The `<showtech file>` must have a `.tar.xz` extension.
- Do not use quotation marks for filenames.
- On a Mac operating system, use OpenSSL 1.1.1+ since LibreSSL is not supported.

The decrypted metrics file is available for use or analysis.

Download the showtech logs

Download encrypted showtech logs for all collection jobs from a Data Gateway instance.

You may need to retrieve showtech logs from a Data Gateway for troubleshooting or support analysis. This task explains how to use the Cisco Crosswork UI to securely download the showtech logs. The logs are encrypted and requires a passphrase for decryption.

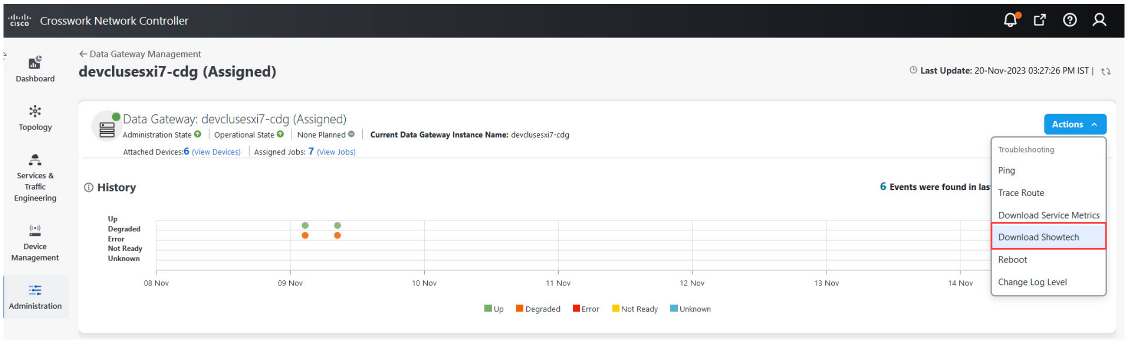
Procedure

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 Data Gateway details page, at the top-right corner, click **Actions** > **Download Showtech**.

Figure 39: 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
Troubleshooting
Ping
Trace Route
Download Service Metrics
Download Showtech
Reboot
Change Log Level
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
Up
Degraded
Error
Not Ready
Unknown

Step 4 Enter a passphrase.

Note
Ensure that you make a note of this passphrase. This passphrase is used later to decrypt the file.

Step 5 Click **Download Showtech**.

The file is downloaded to the default download folder on your system in an encrypted format.

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

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<password>
```

Example:

```
openssl enc -d -aes-256-ctr -pbkdf2 -md sha3-512 -iter 100000 -in show-tech-file.tar.xz.enc -out
show-tech-file.tar.xz -pass pass:myPassword
```

Note

- Use OpenSSL version 1.1.1i to decrypt the file. To check the OpenSSL version on your system, use the command `openssl version`.
- The `<showtech file>` must have a `.tar.xz` extension.
- When referring to the `<showtech file>` and `<decrypted filename>`, do not enclose the filenames in quotation marks.
- To decrypt on a MAC, you need OpenSSL 1.1.1+, as LibreSSL does not support all the necessary switches.

After completing this task, you will have securely downloaded encrypted showtech logs for all collection jobs from the selected Data Gateway instance. You can use your passphrase to decrypt the downloaded file and review logs for troubleshooting or support analysis. The decrypted metrics will be available in your system's default download folder.

Reboot Data Gateway VM

Restart a data gateway virtual machine to restore or refresh its services.

Perform this task from the Crosswork Network Controller UI. When you reboot the data gateway, its functionality is paused until the VM is running again.

Before you begin

Be aware that rebooting the Data Gateway pauses its functionality until the virtual machine restarts.

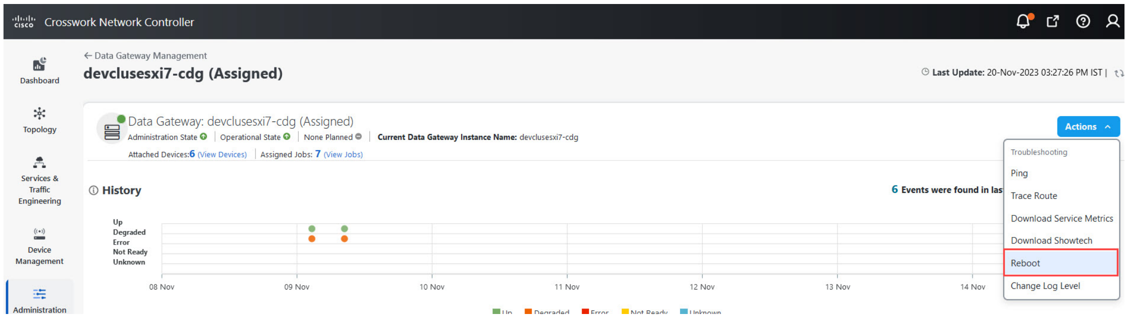
Procedure

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

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

Step 3 On the **Crosswork Data Gateway details** page, at the top-right, click **Actions**, then click **Reboot**.

Figure 40: Data Gateway reboot



devclusesxi7-cdg (Assigned)

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

Data Gateway: devclusesxi7-cdg (Assigned)

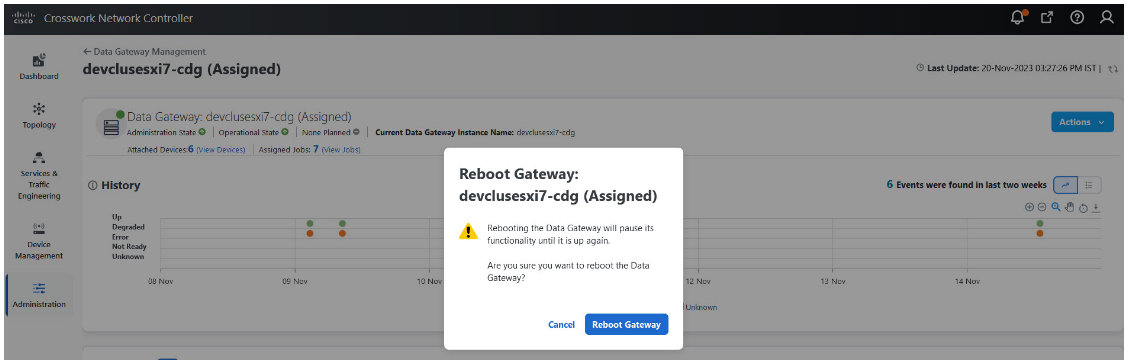
Administration State | Operational State | None Planned | Current Data Gateway Instance Name: devclusesxi7-cdg

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

6 Events were found in las

Step 4 Click **Reboot Gateway** to confirm.

Figure 41: Reboot Data Gateway pop-up



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 the log level of components

This document provides step-by-step instructions for users to change the log level of specific components in a Crosswork Data Gateway through the Cisco Crosswork UI.

Changing the log level allows users to adjust the verbosity of logs generated by individual components, such as collectors and infrastructure services, on a targeted Crosswork Data Gateway. The procedure limits log level changes to the Data Gateway selected by the user and ensures accurate configuration for troubleshooting or monitoring purposes. The instructions are intended for administrators managing data gateways within the Cisco Crosswork platform.

Procedure

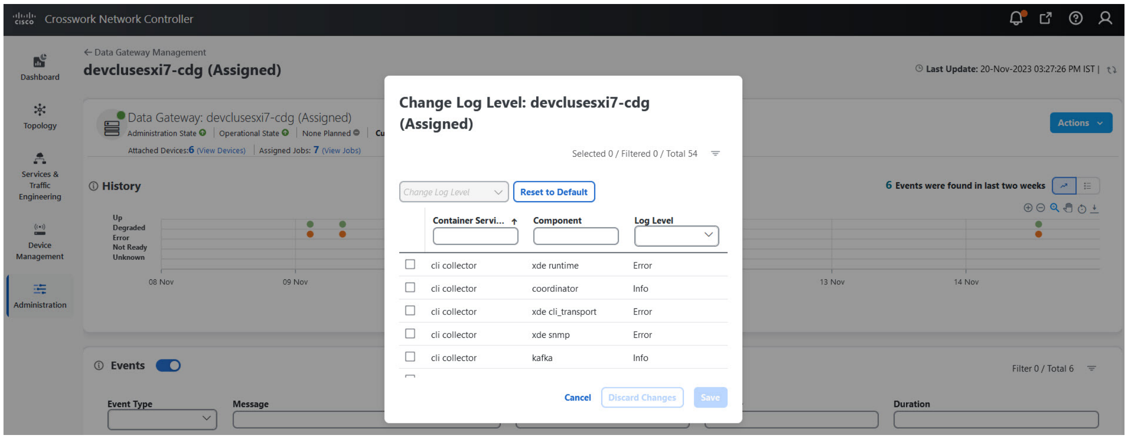
Step 1 Go to **Administration** > **Data Gateway Management** > **Data gateways**.

Step 2 Click the Data Gateway name where you want to change the log level for collectors of Crosswork Infrastructure services.

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

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

Figure 42: Change log level



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
Actions
History
Events
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 At the top of the table, open the **Change Log Level** drop-down list and select a log level: Debug, Trace, Warning, Info, or Error.

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

Step 6 Click **Save**.

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

Troubleshooting common issues

This section provides information about the common troubleshooting issues that you might face when using Data Gateway.

Use this section to access topics related to common issues in Crosswork Data Gateway.

- Troubleshoot Data Gateway not moving from assigned to unassigned state issue, on page 109
- Resolve incorrect NLB health report for active Data Gateway, on page 109
- Recover collection job from degraded state, on page 110
- Resolve Data Gateway collection issue after SNMPv3 engine ID update, on page 110
- Recover LVPN service from monitoring initiated state, on page 110
- Resolve missing IPv6 address and port details in error message, on page 111
- Handle DAD error in Data Gateway failover process, on page 111
- Resolve Data Gateway failover issues, on page 112

Troubleshoot Data Gateway not moving from assigned to unassigned state issue

This procedure describes how to remove a Data Gateway from an HA pool when it remains in the Assigned state. Use these steps to ensure the Data Gateway can be safely removed while maintaining high availability and proper pool operation.

On the **Create Pool** page, within the **Add Data Gateway instance to pool** pane, some Data Gateways in the Assigned state cannot be moved to the Unassigned state, even if they do not have any devices attached. This situation typically means the Data Gateway has a virtual IP assigned, which prevents its removal from the HA pool using standard actions.

Before you begin

Use these steps to remove a Data Gateway out of the HA pool while it is in the **Assigned** state.

Procedure

Step 1 Add an additional Data Gateway to the HA pool only if a spare is not already present.

Step 2 Perform a manual failover to make the assigned Data Gateway a spare.

Step 3 Update the HA pool to reduce the spare count, then move the spare Data Gateway out of the pool.

What to do next

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 Data Gateway, see *Delete Crosswork Data Gateway Instance from Cisco Crosswork*.

Resolve incorrect NLB health report for active Data Gateway

This procedure helps you identify and resolve incorrect Network Load Balancer (NLB) health reports for an 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.

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.

Recover collection job from degraded state

This task guides administrators on how to recover a collection job when it enters a degraded state, ensuring continued data collection and system reliability

A collection job may enter the Degraded state on the Collection Jobs page, indicating potential issues with service status or system components. By reviewing the service status and identifying the responsible collector, administrators can diagnose the cause of degradation and apply corrective actions. Access to administrative tools and navigation through the Data Gateway Management interface are required to complete these procedures.

Before you begin

Use these steps if the collector is not listed in the Service status section.

Procedure

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

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

Step 3 When the confirmation message is prompted, click **Yes**.

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

Resolve Data Gateway collection issue after SNMPv3 engine ID update

Describe how to resolve a Crosswork Data Gateway collection issue that occurs after an SNMPv3 engine ID update, including the underlying system behavior and recommended workaround actions to restore appropriate data collection.

When the SNMPv3 engine ID changes or the device experiences downtime or reachability issues, the SNMP collector continues collecting data. The data gateway should pause collection when these changes occur. Data collection continues even when the Force Re-Sync USM Engine Details for SNMPv3 option is disabled.

Workaround: 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 Data Collector(s) Global Settings*.

Recover LVPN service from monitoring initiated state

This document explains how to recover an LVPN service that is stuck in the monitoring initiated state. It describes the cause of the issue, when the device fails to connect properly to the Data Gateway, and outlines steps to resume data collection by detaching and reattaching devices through Crosswork Data Gateway.

If the device cannot establish a connection with Data Gateway, the gNMI collection job fails with an error. The L2VPN Point to Point service is then unable to monitor the devices, and the status in the Crosswork UI shows Monitoring initiated.

Workaround: To resume data collection, detach, and then reattach the devices using Crosswork Data Gateway.

For more information, see:

- Reattach the devices: *Attach devices to a Data Gateway*
- Detach the devices: *Manage Crosswork Data Gateway device assignments*

Resolve missing IPv6 address and port details in error message

Help users identify and resolve cases where IPv6 address and port details are missing or displayed in a combined format within device error messages on the Crosswork Network Controller.

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.

Workaround: When troubleshooting devices with an IPv6 address, the message displays the address and port number 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. If the IP address contains only eight segments, the port number is unavailable.

Handle DAD error in Data Gateway failover process

Resolve a persistent Duplicate Address Detection (DAD) error that may occur during the failover process between Data Gateway instances. The steps ensure that the Data Gateway transitions to the UP state by clearing the DAD error when automatic resolution does not occur in the expected timeframe.

During a Data Gateway failover, the secondary Data Gateway inherits the southbound IPv6 address that was previously assigned to the primary Data Gateway. This inheritance can cause the operating system to register a DAD error, as the address was initially tied to the primary instance. Crosswork detects this condition, logs a DAD failure event, and, under normal circumstances, the error self-resolves within approximately 5 minutes. If the DAD error persists beyond this period, manual intervention is required to clear the DAD flag and bring the Data Gateway back to the UP state.

Note This behavior is expected and usually resolves within 5 minutes.

Once the DAD failure status is cleared by the operating system, Crosswork automatically transitions the Data Gateway to the UP state.

Before you begin

Workaround: Use these steps if the DAD failure error persists for more than 5 minutes.

Procedure

Remove the southbound VIP address from the secondary Data Gateway and reassign it using these commands.

a) Delete the VIP address.

```
ip address del {southbound_ip}/{mask} dev eth2
```

b) Replace the VIP address.

```
ip address replace {southbound_ip}/{mask} dev eth2
```

What to do next

-

Resolve Data Gateway failover issues

Provide guidance on resolving Data Gateway failover issues by outlining necessary steps to reattempt failover and ensure standby instances are in the correct operational state.

Workaround: 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.

Wait 10 to 30 seconds for the standby data gateway to move to the NOT_READY state before initiating a subsequent failover. If the standby instance remains in the UP state after 30 seconds, restart the oam-manager of the data gateway. This action restores the operational state to NOT_READY.