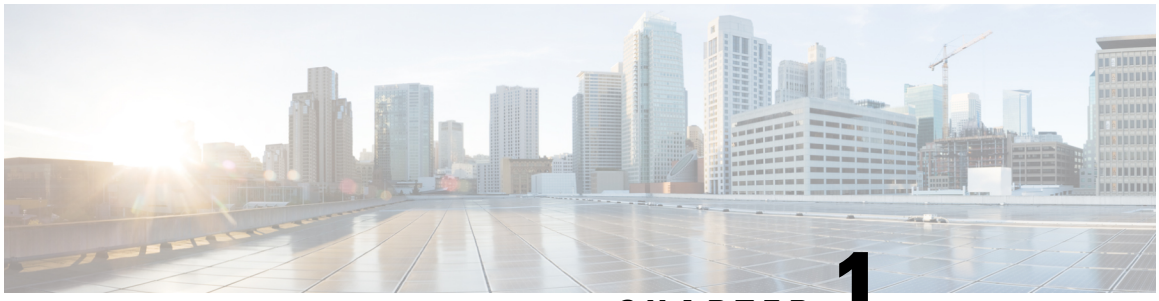
Cisco Crosswork Network Controller 7.2 Administration Guide

First Published: 2026-01-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Set Up Crosswork Network Controller

Use the following topics to set up, configure, and access Crosswork Network Controller after installation.

Core features in Crosswork Network Controller

Familiarize yourself with the fundamental features essential for understanding and using Cisco Crosswork Network Controller.

Table 1: Core features in Crosswork Network Controller

Feature	Description
User roles	Use role-based access control to allow each user to access only the software functions needed for their job duties. New users start with full administrative privileges. To grant only the necessary privileges, create user roles and assign the appropriate roles to each user profile.
User accounts	Create separate accounts for each user to maintain a detailed audit record of user activity. Prepare a list of users, decide on usernames and temporary passwords, and create user profiles for each account. You can use TACACS+, LDAP, or RADIUS servers to centrally manage user roles and accounts. For more details, see *<xref to AAA section>* .
Device-access groups	Device-access Groups (DAGs) are groups of devices that define device access for users. Users associated with DAGs can make configuration changes and provision services on devices within those groups. When creating a user, assign at least one DAG and a role to the user. For more details, see *<xref to DAG section>*.

Feature	Description
Credential profiles	For the Crosswork Network Controller to access a device or interact with a provider, it must present credentials. Instead of entering credentials each time, you can create credential profiles to securely store this information. The platform supports unique credentials for each access protocol and allows bundling multiple protocols and their corresponding credentials into a single profile. Devices using the same credentials can share a credential profile. For example, if all routers in a particular building share a single SSH user ID and password, you can create one credential profile for Crosswork Network Controller to manage them. Before creating a credential profile, gather the access credentials and supported protocols needed to monitor and manage your devices. These credentials include user IDs, passwords, SNMPv2 read and write community strings, and SNMPv3 authentication and privilege types. For other providers (NSO, SR-PCE, Storage, Alert, and WAE), you always need user IDs, passwords, and connection protocols. Use this information to create credential profiles.
Tags	Tags are simple text strings that you can attach to devices to help group them. The Crosswork Network Controller includes a short list of pre-made tags for grouping network devices. You can also create your own tags to identify, find, and group devices for various purposes. Plan a preliminary list of custom tags to create when setting up the system. Use these tags to group your devices when you first onboard them. You can always add more tags later, so a complete list is not necessary at the start. Add all planned tags before they are needed. If any tags are missing, add them manually at that time. For more details, see *<xref to Tags section>*.

Feature	Description
Providers	Crosswork Network Controller applications rely on external services like Cisco Crosswork Network Services Orchestrator (NSO) or SR-PCE for tasks such as configuration changes and segment routing path computation. To manage access and reuse information between Crosswork Network Controller applications, configure a provider (for example, NSO or SR-PCE) for each external service. The provider family determines both the type of service supplied to Crosswork Network Controller and the unique parameters required for configuration. The parameters needed to configure a provider depend on the type of Crosswork Network Controller application used. It is important to review and gather each application's requirements before configuring a provider. For more information, see *<xref to Provider families>* and *<xref to provider dependency matrix>*. The main providers used with Crosswork Network Controller are: • Cisco Crosswork Network Services Orchestrator (NSO) is used by many Crosswork Network Controller applications to make changes to device configurations and provision services on devices. To add NSO as a provider, you need the IP address and credentials used for communication. For more details, see *<xref to NSO providers>*. **Note** Additional steps are required when using NSO in LSA mode. For more details on these steps, see *<xref to Enable LSA topic>*. • If you plan to use Crosswork Optimization Engine, at least one Cisco SR-PCE provider must be defined to discover devices and distribute policy configurations to devices. Additional SR-PCEs can be used for more complex network topologies and redundancy. You can manually add devices to the system or auto-onboard them using SR-PCE discovery. Decide on your process for deployment and configuration before making configuration changes.
Devices	You can onboard devices using the UI, a CSV file, an API, SR-PCE discovery, or zero-touch provisioning. The onboarding method determines the type of information needed to configure a device in Crosswork Network Controller. Also, Crosswork Network Controller can forward device configuration to NSO, which may affect how you provision an NSO provider. For more information, see *<xref to Onboarding chapter intro>*. **Note** For information on device configuration, device monitoring, and device management workflows, see the *Crosswork Network Controller 7.2 Device Lifecycle Management* guide.
External data destinations	Crosswork Network Controller functions as the controller for the Crosswork Data Gateway. Operators planning to have Crosswork Data Gateway forward data to other data destinations must understand the format required by those destinations and other connection requirements.

Feature	Description
Labels	If you plan to use Change Automation, labels are used to restrict which users can execute a playbook. For example, you may allow lower-level operators to run check playbooks but use labels to prevent them from running more complex or impactful playbooks that make changes to network device configurations.
KPI profile	If you plan to use Crosswork Health Insights, use KPI (Key Performance Indicator) profiles to monitor network health. You can establish unique performance criteria based on how a device or devices are used in the network. KPIs can be grouped to form a KPI Profile. It is helpful to have a clear idea of the data you plan to monitor and the performance targets you want to establish as you set up Health Insights.
Device monitoring samples	If you plan to install the Crosswork Service Health application, you should review the provided samples to determine if they are adequate for monitoring devices in your network.

Note that you can capture the devices, credential profiles, tags, and providers lists in spreadsheet form, convert the spreadsheet to CSV format, and then upload them in bulk to the Crosswork Network Controller application using the Import feature. You can access CSV templates for each of these lists by clicking the Import icon in the corresponding places in the user interface. Select the **Download template** link when prompted to choose an export destination path and filename.

Tasks to complete for initial setup

This topic guides you through preparing the system for use when deploying Crosswork Network Controller, whether as a cluster or a single VM.

This table lists the topics to refer to for assistance when performing each of the following tasks. If you have completed the recommended planning steps outlined in the *<xref to Core components topic>*, you should have all the information required to complete each step in this workflow.

Note This workflow assumes that you have already installed Crosswork Network Controller based on the instructions in the latest version of the *Cisco Crosswork Network Controller 7.2 Installation Guide* .

Table 2: Tasks to complete to get started with Crosswork Network Controller

Step	Action
1. Ensure that your devices are configured properly for communication and telemetry.	Refer to the guidelines and sample configurations in *<xref to config prereq samples>*.
2. Create user accounts and user roles.	Follow the steps in *<xref to Manage Users section>* and *<xref to Create user roles>*.
3. Create credential profiles.	Follow the steps in *<xref to Create credential profiles>*.

Step	Action
4. Add the provider(s).	Follow the steps in *<xref to Add provides through UI>*. **Note** In case of the single VM deployment of Crosswork Network Controller Advantage tier, the embedded NSO provider is already added and configured during the deployment.
5. Validate communications with the provider(s).	Check on the provider's reachability using the steps in *<xref to View provider details>*.
6. Import or create tags.	To import them: *<xref to Import tags>*. To create them: *<xref to Create tags>*.
7. Onboard your devices.	See *<xref to Onboard intro>*. For more information, see the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management* guide.
8. Setup Crosswork Data Gateway	For cluster deployment, follow the steps in *<xref to CDG cluster chapter>*. For single VM deployment, follow the steps in *<xref to CDG SVM chapter>*.
9. Validate Crosswork Network Controller communications with devices.	Review the **Devices** window. All the devices you have onboarded should be reachable. Click ⓘ to investigate any device whose **Reachability State** is marked as (unreachable), (degraded), or (unknown). For more information, see the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management* guide.
10. (Optional) Enable source IP for auditing.	If you want to log the user's IP address for auditing and accounting, see *<xref to AAA section>*.
11. (Optional) Create additional user accounts and user roles.	Follow the steps in *<xref to Manage Users section>* and *<xref to Create user roles>*.
12. (Optional) Import or create additional credential profiles and providers.	To import providers: *<xref to Import providers>*. To create providers: *<xref to Add providers through UI>*.
13. (Optional) Group your devices logically as per your requirement.	Follow the steps in *<xref to Use device group to filter topology map>*.
14. (Optional) Set display preferences for your topology.	Follow the steps in *<xref to Work offline internal maps>* and *<xref to Show link utilization by color>*.

Log in to Crosswork Network Controller

Access the Crosswork Network Controller and manage your account session securely and efficiently.

Crosswork Network Controller provides a browser-based user interface. Security and usability features such as session lockouts, color themes, and password management ensure robust user experience.

Attention The number of unsuccessful login attempts and lockout timing is set by an administrator in Local Password Policy. For details on lockout settings, see Configure AAA settings, on page 449.

Before you begin

- Use a supported browser version. See the *Compatibility Information* section in the *Release Notes for Crosswork Network Controller, Release 7.2.0*.
- Obtain your login credentials. The default administrator username is `admin`; its password must be changed at installation.
- The login page is inaccessible if the Central Authentication Service (CAS) pod is restarting or not running.

Procedure

Step 1 **Log in**

a) Open a supported web browser.

b) Enter one of the following URLs to access the Crosswork Network Controller:

- For IPv4: `https://<Crosswork Management Network Virtual IP (IPv4)>:30603/`
- For IPv6: `https://[<Crosswork Management Network Virtual IP (IPv6)>]:30603/`

Note
IPv6 addresses must be enclosed in brackets.

c) If accessing for the first time, your browser may display a warning that the site is untrusted.

Follow prompts to add a security exception and download the self-signed certificate, after which future logins are trusted.

d) The login window appears. Enter your username and password.

Note
- The administrator account (`admin`) is created at installation. Its password must be changed during installation verification.
- Cisco strongly recommends keeping default administrator credentials secure. Do not use the default admin account for routine logins; instead, create user roles with required privileges and assign users accordingly. At least one user should have the **admin** role.

e) Click **Login**.

Note
Be aware: Repeated unsuccessful login attempts result in account lockout, as configured by your administrator in the **Local password policy**. After account lockout, wait until the configured time elapses, then log in with valid credentials.

Step 2 **Change password**

a) At any time after logging in, click the icon in the top right corner of the main window.
b) Select **Change password**.
c) In the dialog box, enter your current password and new password.
d) Click **Change password** to confirm the update.

Note
If you need to update the HTTPS (UI admin login) password for the cluster:

- Update the HTTPS (UI admin login) password at the cluster level, ensuring that the new password applies to the entire cluster rather than to individual nodes.
- After you update the HTTPS password at the cluster level, immediately update the same password in the geo inventory to maintain consistency and ensure proper authentication across the system.

Step 3 **Set color theme**

a) Click the icon in the top right corner.
b) Choose either **Classic light** or **Classic dark** from the color theme options.

Note
By default, **Classic light** is selected.

Step 4 **Log out**

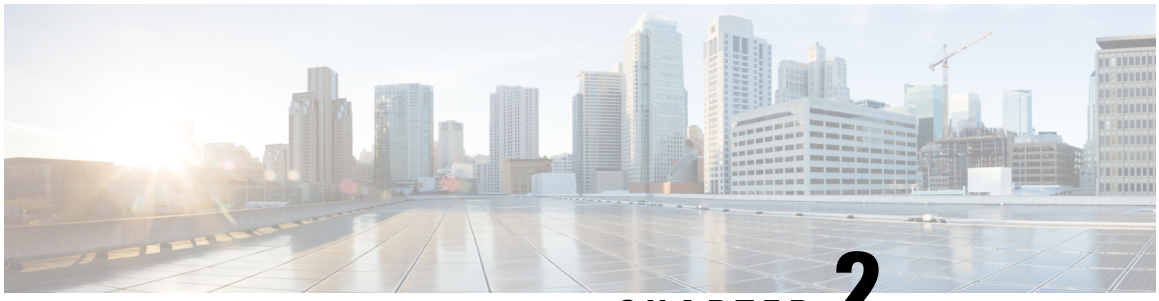
a) Click the icon in the top right corner.
b) Select **Logout**.

- If you have multiple sessions open from the same client (across multiple browser tabs/windows) and log out or terminate a session in one tab/window, only the tab/window where logout was performed displays the logout screen.
- All other tabs/windows show the error message: "`Your session has ended. Log into the system again to continue.`"

You have securely logged in to Crosswork Network Controller, managed your credentials, customized your color theme, and logged out. All personal session data is protected and terminated as required.

What to do next

If you changed your password, ensure you remember your new credentials. After logging out, close all browser tabs or windows to fully terminate access.



CHAPTER 2

Manage Backup and Restore

Use this chapter for guidance on protecting your Crosswork Network Controller data and system configurations. Find essential procedures and reference information for backing up, restoring, and recovering your environment.

Backup and restore features

Backup and restore features are application functions that

- help prevent data loss,
- preserve installed applications and settings, and
- provide options to back up external data.

To access these features, from the main menu, click **Administration** > **Backup and Restore** to open the **Backup and Restore** window.

Among the backup options, you can also choose to **Backup NSO**. This option preserves the external NSO data along with the Crosswork Network Controller configuration.

Backup and restore options

Crosswork Network Controller offers multiple menu options to backup and restore your data.

Table 3: Backup and restore options

Menu option	Description
Actions > **Data Backup** (See Back up data, on page 12 for details)	Preserves the Crosswork Network Controller configuration data. The backup file can be used with the data disaster restore (Restore data after a disaster, on page 14) to recover from a serious outage.
Actions > **Data Disaster Restore** (See Restore data after a disaster, on page 14 for details)	Restores the Crosswork Network Controller configuration data after a natural or human-caused disaster has required you to rebuild a Crosswork cluster. First, deploy a new cluster by following the instructions in the *Cisco Crosswork Network Controller 7.2 Installation Guide*. Ensure you install the exact versions of the applications that were in your old Crosswork cluster when you made the data backup. Any version mismatch can lead to data loss and restore job failure.
Actions > **Data Migration** (See Migrate data using backup and restore, on page 19 for details)	Migrates data from an older version of Crosswork Network Controller to a newer version.

Supported backup and restore combinations

Crosswork Network Controller supports these backup and restore combinations.

Table 4: Supported backup and restore combinations

Backup type	From deployment	To deployment	Support
Data only	Geo redundant	Geo redundant	Supported only on the active cluster
Data only	Non-geo redundant	Non-geo redundant	Supported

Any other combination is not supported.

Embedded NSO backups

An embedded NSO backup is a data protection mechanism that

- is automatically included when the Crosswork Network Controller Advantage package is deployed on a single VM,
- always backs up the embedded NSO as part of the main backup operation without separate workflows or exclusion options, and

- includes the embedded NSO data within the primary backup tar file.

Additional information

- The embedded NSO cannot be excluded during backup or restore operations, unlike an external NSO.
- There is no specific option in the UI to enable/disable Backup NSO for embedded NSO.
- Embedded NSO is currently not included during the data migration between different Crosswork Network Controller release versions.
- When installed, the embedded NSO automatically onboards an NSO provider entry and an SSO service provider entry with cross-launch support, which cannot be edited or deleted; if removed, the system reinstates them upon restart.
- Any data configured on a device after a backup operation will not be in sync with NSO once the restore operation is completed. You must perform a check sync on the device to obtain the correct status before initiating the restore operation.

Requirements for backup and restore

These items define the mandatory conditions and limitations that must be met for successful backup and restore operations for a Crosswork Network Controller cluster.

- Configure a destination SCP server for storing backup files during your first login. This is a one-time setup and must be completed before taking backups or initiating restore operations.
- Use the same platform image for disaster restore as was used for creating the backup. Different software versions are not compatible for disaster restores.
- Only one backup or restore operation can run at a time.
- Ensure both the Crosswork Network Controller cluster and the SCP server are in the same IP environment (e.g., both using IPv6).
- By default, backups are not allowed if the system is not considered healthy, but this can be overridden for troubleshooting purposes.
- Export the cluster inventory file when performing a data backup.
- If Crosswork Network Controller is reinstalled after a disaster and Data Gateways are enrolled before the restore, a certificate mismatch may occur. To fix this, re-import the certificates from the **Change Current System Settings** menu on the Crosswork Data Gateway VM.

Best practices for backup and restore

These items outline suggested actions that help ensure smoother, safer, and more efficient backup and restore processes for a Crosswork Network Controller cluster.

- Perform backup or restore operations during a scheduled maintenance window. Users should not access the system during these operations. Backups will take the system offline for about 10 minutes, while restore operations can be lengthy and pause other applications, affecting data-collection jobs.

- Use the dashboard to monitor the progress of backup or restore processes. Avoid using the system during these processes to prevent errors or incorrect content.
- Operators are responsible for periodically deleting older backups from the target server to ensure adequate storage for new backups, as Crosswork Network Controller does not manage them. Deleted backups may still appear in the job list.
- Operators making frequent changes should back up more often (possibly daily), while others might back up weekly or before major system upgrades.

Back up data

This task describes how to perform a data backup operation from the Crosswork Network Controller UI.

The backup process depends on having SCP access to a server with sufficient storage space. The storage required for each backup varies based on your cluster size, applications in the cluster, and scale requirements. The time taken for the backup process also varies based on the type of backup, cluster size, and applications.

Note Building a target machine for the backup is out of scope for this document. The operator is expected to have the server in place, know the server credentials, and have a target directory with adequate space for the backups.

Before you begin

Before you begin:

- Ensure you have a secure SCP server in place, with adequate space for backups. Building the target machine is out of scope for this document.
- Obtain the hostname or IP address and port number of the SCP server, a file path on the server for backup files, and user credentials with read and write permissions to that path.
- If you want to include external NSO data in the backup process, follow the instructions in Back up data using external NSO, on page 15 instead of the instructions in this topic.

Procedure

Step 1 Go to **Administration** > **Backup and Restore**.

Step 2 Configure the SCP backup server destination:

a) Click **Destination**.
b) In the **Add Destination** dialog box, enter the hostname, port, destination path, and credentials for the SCP server.
c) Click **Save** to confirm the configuration.

Step 3 Create a backup job:

a) Click **Actions** > **Data Backup**.
b) In the **Data Backup** dialog box, Provide a relevant name in the **Job name** field.
c) (Optional) Check the **Force** checkbox to create the backup despite any application or microservice issues.
d) (Optional) Uncheck the **Backup NSO** checkbox if you do not want to include external NSO data in the backup.

To use the **Backup NSO** option, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail. This option is not applicable for single VM deployments.

e) Complete any remaining fields as needed. To specify a different remote server upload destination, edit the **Host name**, **Port**, **Username**, **Password**, and **Path** fields.
f) (Optional) Click **Verify backup readiness** to confirm sufficient resources for the backup. If successful, click **OK** to acknowledge the warning about the operation's duration.
g) Click **Backup** to start the backup.

Step 4 Monitor the backup progress in the **Job details** panel.

The system creates a backup job set and adds it to the job list. The **Job details** panel reports the status of each backup step.

If the backup fails during upload to the remote server, investigate and resolve the issue (e.g., incorrect credentials, invalid destination directory, or lack of space). Then, in the **Job details** panel, click the **Upload backup** button to retry the upload.

The system creates and uploads a backup to the specified SCP destination. The backup job appears in the job list with status detail.

What to do next

Keep the build versions and backup files in a safe location for future restores.

Restore data

This task describes how to perform a data restore operation from the Crosswork Network Controller UI.

The time taken for the restore process varies based on the type of backup, your cluster size, and the applications in the cluster.

Before you begin

Before you begin:

- Ensure you have a backup file available for restore.
- You must install the exact build versions of the applications that were present when the backup was created. Any mismatch can result in data loss and failure of the data restore job.

Procedure

Step 1 Go to **Administration** > **Backup and Restore**.

Step 2 Select the backup file for restore:

a) In the **Backup and Restore Job Sets** table, select the data backup file you want to use for the restore. The **Job details** panel displays information about the selected backup file.
b) Click the **Data restore** button to start the restore operation.

Step 3 Monitor the restore progress:

The system creates a restore job set and adds it to the job list. To view the progress, click the link to the progress dashboard.

Attention
If MDT (Model-driven Telemetry) collection jobs were deleted after the backup, the restore operation will fail to recover them, leaving them in an error state due to missing device configurations. To rectify this, perform ONE of the following actions:

- Restore the backup taken for external NSO (only applicable if the original backup included external NSO).
- Move the devices associated with MDT collection DOWN and UP in Device Management.
- Detach and attach devices to the Crosswork Data Gateway pool.

Note
In a geo-redundant setup, if external destinations are added and Data Gateway is re-enrolled after a backup, restoring the backup file may result in stale certificate expiry alarms. These alarms must be manually cleared.

The system initiates the restore operation from the selected backup file. The restore job appears in the job list with status detail.

Restore data after a disaster

Use this task when the original Cisco Crosswork cluster has been destroyed due to a natural or human-caused disaster. A new cluster must be deployed with the same configuration as the original before restoring data.

Before you begin

Before you begin:

- Obtain the full name of the backup file from the SCP backup server (typically the most recent backup). Backup filenames follow this format: `backup_JobName_CWVersion_TimeStamp.tar`.
  - *JobName* is the user-entered name of the backup job.
  - *CWVersion* is the platform version of the backed-up system.
  - *TimeStamp* is the date and time when backup file was created.

  Example: `backup_Wednesday_7-2_2026-01-25-12-00.tar`.
- Ensure the new cluster uses the exact versions of all applications and the platform as the original cluster. Any mismatch can cause data loss or restore failure.
- Use the same IP addresses, number and types of nodes, and software image as the original cluster. Internal certificates depend on these details.
- Keep backups current. If you installed new applications or patches since the last backup, create a new backup.
- If only a single hybrid node or one or more worker nodes are malfunctioning, do not perform disaster recovery. Use cluster management features to replace or redeploy these nodes. If multiple hybrid nodes are malfunctioning and the system is nonfunctional, deploy a new cluster and restore using a recent backup.

- Smart licensing registration for applications is not restored and must be registered again after the restore.
- If recovery fails, contact Cisco Customer Experience for assistance.
- After restore, use the Configuration Database CLI tool to identify and reload any missing SR policies or RSVP-TE tunnels. See Orphaned SR-TE policies and RSVP-TE tunnels, on page 20 for more details.

Procedure

Step 1 Deploy a new cluster as described in the *Cisco Crosswork Network Controller 7.2 Installation Guide*.

Step 2 From the main menu, go to **Administration** > **Backup and Restore**.

Step 3 Click **Actions** > **Data Disaster Restore** to open the **Data Disaster Restore** dialog.

Step 4 In the **Backup File Name** field, enter the backup file name to restore.

Step 5 Click **Start Restore**.

To monitor progress, use the progress dashboard link.

The new cluster restores its data from the specified backup file. The configuration and data state return to the point of the last backup.

What to do next

- Re-register smart licensing for all restored applications.
- Use the Configuration Database CLI to identify and reload any missing SR policies or RSVP-TE tunnels.

Back up data using external NSO

Create a backup of your Crosswork data, optionally including the NSO CDB, to a remote SCP server.

Backing up Crosswork and NSO data ensures you can recover configurations in case of system issues. NSO backups can be automated, but restoring the NSO CDB is a manual process. For restore instructions, see Restore data using an external NSO, on page 17.

Before you begin

Ensure that you:

- Install a compatible version of NSO in system default mode.
- Install the latest version of the Crosswork Network Controller Transport SDN function pack using the **NSO deployment manager** window. For more information, see *Install Cisco NSO Function Pack Bundles from Crosswork UI* in the *Crosswork Network Controller 7.2 Installation Guide*.
  - If you did not install the Transport SDN Function Pack using the **NSO deployment manager** window and instead installed it manually, you must manually copy the `ncs_backup.sh` script into the `/var/opt/ncs/scripts` folder. Otherwise, the backup operation will fail.
    1. Get the NCS run directory using the command: `vi $NCS_DIR/../installdirs`

Example: `NCS_RUN_DIR="/var/opt/ncs"`

2. Copy the scripts to the NCS run directory.

```
$ cd tsdn-<RELEASE-VERSION>-nso-<NSO-VERSION>/
$ sudo cp ncs_backup.sh <NCS_RUN_DIR>/scripts/
$ sudo cp ncs_restore.sh <NCS_RUN_DIR>/scripts/
```

Example:

```
$ sudo cp ncs_backup.sh /var/opt/ncs/scripts/
$ sudo cp ncs_restore.sh /var/opt/ncs/scripts/
```

- Collect the hostname or IP address, port number, and file path for your SCP server.
- Ensure you have SCP server credentials with read and write access to the backup folder.
- Configure SSH as the connectivity protocol in the NSO provider, with an appropriate credential profile.
- Ensure the user associated with the credential profile has sudo permissions and full access to `/var/opt/ncs/backups/` on the NSO server.
- See general backup guidelines in Back up data, on page 12 for additional requirements.

Note If any prerequisite is not met, the backup job may fail.

Procedure

Step 1 Configure the SCP backup server.

a) Go to **Administration** > **Backup and Restore**.
b) Select **Destination** and enter the required backup server details.
c) Click **Save** to confirm the configuration.

Step 2 Create a backup job for Crosswork and external NSO data.

a) In **Administration** > **Backup and Restore**, select **Actions** > **Backup**.
b) Enter a job name in the **Job Name** field.
c) (Optional) Select **Force** to allow backup if there are application or microservice issues.
d) Ensure **Backup NSO** is checked.
e) Complete remaining fields as needed. To change the upload destination, edit the **Destination** settings.
f) Click **Start Backup** to begin the operation.

Step 3 Monitor the backup job.

a) View the job in the **Backup Restore Job Sets** table. Click on the job set to see status and details in the **Job Details** panel.
b) If an upload to the SCP server fails, click **Upload backup** in the **Job Details** panel to retry. To change the destination, edit **Destination** settings before retrying.

A backup of Crosswork and (optionally) NSO data is created and stored on the SCP server. The job status and any errors are displayed in the Job Details panel.

What to do next

- For restoration, see Restore data using an external NSO, on page 17.
- Review backup jobs to confirm successful completion.

Restore data using an external NSO

Restore a Crosswork cluster and its associated NSO from a backup file located on an SCP server.

Use this task to recover your Crosswork cluster and NSO in the event of data loss or system migration. Perform this operation during a scheduled maintenance window only. Do not allow users to access Crosswork or NSO while the restore is in progress. The operation may be lengthy and will pause other Crosswork applications until complete. NSO must be completely stopped during the restore process.

Note Restoring from the external NSO backup file is a manual process.

Before you begin

Before you begin:

- Obtain the full name of the backup file from the SCP backup server (typically the most recent backup). Backup filenames follow this format: `backup_`*`JobName`*`_`*`CWVersion`*`_`*`TimeStamp`*`.tar`.
  - *JobName* is the user-entered name of the backup job.
  - *CWVersion* is the platform version of the backed-up system.
  - *TimeStamp* is the date and time when backup file was created.

  Example: `backup_Wed_7-2_2026-01-25-12-00.tar`.
- Ensure that NSO is not running before you begin the restore operation.

Procedure

Step 1 Log in to the remote SCP backup server. Access the backup destination directory and locate the backup file containing external NSO information.

```
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_7-2_2026-01-25-12-00.tar
```

Step 2 Extract the NSO backup from the main backup file using `tar -xvf`.

```
[root@localhost~]# tar -xvf ackup_Wed_7-2_2026-01-25-12-00.tar
...
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_7-2_2026-01-25-12-00.tar
-rw-r--r--. 1 root root 8267798605 468c4715-ea09-4c2b-905e-98999d.tar
```

Step 3 Extract the NSO backup file in the destination folder.

This will create a folder structure under `/nso/ProviderName/`, where *ProviderName* is the configured NSO provider name.

In the following example, the NSO provider is named `nso121`:

```
tar -xvf 468c4715-ea09-4c2b-905e-98999d.tar
468c4715-ea09-4c2b-905e-98999d/nso/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/log/
468c4715-ea09-4c2b-905e-98999d/nso/nso121/log/nso_backup_result_nso121_Wed.log
468c4715-ea09-4c2b-905e-98999d/nso/nso121/NSO_RESTORE_PATH_nso121
468c4715-ea09-4c2b-905e-98999d/nso/nso121/ncs-5.4.2@backup_Wed_nso121.backup.gz
...
```

Step 4 Locate the file with a `.backup.gz` extension in the `/nso/ProviderName/` folder. This is the generated NSO backup file.

Step 5 Log in to NSO as a user with root privileges. Copy or move the generated NSO backup file from the SCP server to the restore path location of the NSO cluster.

```
[root@localhost nso121]# more NSO_RESTORE_PATH_nso121/var/opt/ncs/backups/

[root@localhost nso121]# ls
log ncs-5.4.2@backup_Wed_nso121.backup.gz NS0_REST0RE_PATH_nso121
[root@localhost nso121]# more NS0_REST0RE_PATH_nso121
/var/opt/ncs/backups/
[root@localhost nso121]#
...
```

Step 6 Stop NSO before starting the restore operation.

```
$/etc/init.d/ncs stop
```

Step 7 Restore NSO using the backup file.

```
#ncs-backup --restore ncs-5.4.2@backup_Wed_nso121.backup.gz
```

If you encounter issues running this command, ensure you have `sudo su` permission.

Step 8 Restart NSO after the restore completes.

```
$/etc/init.d/ncs start
```

Step 9 Re-add the NSO provider to Crosswork after restoring both Crosswork and NSO clusters from backups.

Complete the NSO configuration to ensure provisioning services function properly. For more information, see Add a Cisco NSO provider, on page 257.

The Crosswork and NSO clusters are restored from backup and ready for continued operation. Services and provisioning can now resume as normal.

What to do next

- Verify that all NSO provisioning services are operational.
- Complete any additional configuration as required for your deployment.

Migrate data using backup and restore

Migrate your data to a new installation or software version using backup and restore operations.

Use this task when upgrading your Crosswork installation to a new software version or moving data to a new installation. Data migration using backup and restore ensures that your configuration and operational data are preserved during transition. Perform these actions during a scheduled maintenance or upgrade window, and ensure users do not access the system during migration.

Before you begin

Before you begin, ensure you have:

- Configured a destination SCP server for storing data migration files (a one-time setup).
- The hostname or IP address and the port number of a secure SCP server.
- A file path on the SCP server to use as the destination for your data migration backup files.
- User credentials for an account with file read and write permissions to the remote path on the SCP server.
- Ensured that the Crosswork cluster and SCP server use the same IP environment (IPv4 or IPv6 as required).
- Captured a screenshot of Data Gateways and recorded their assigned IP addresses and names for redeployment.

Procedure

Step 1 Configure the SCP backup server as your migration destination.

a) In the Crosswork UI, go to **Administration > Backup and Restore**.
b) Open **Destination** and enter the required server details.
c) Save the backup server configuration.

Step 2 Create a migration backup.

a) Log in as an administrator to the Crosswork installation you want to migrate.
b) Go to **Administration > Backup and Restore**.
c) Select **Actions > Data backup** and enter the necessary details, including a job name for the backup.
d) (Optional) Select **Force** to allow backup in case of application or microservice issues.
e) Complete any remaining required fields and adjust the destination if needed.
f) Start the backup operation.
g) Monitor backup progress in the **Backup and Restore Job Sets** table. Review job status and details as needed.
h) If the upload fails, retry using **Upload backup**. Update the destination if required before retrying.

Step 3 Migrate the backup to the new installation.

a) Log in as an administrator on the target Crosswork installation.
b) Go to **Administration > Backup and Restore**.
c) Select **Actions > Data migration** and enter the backup file name to restore from.
d) Click **Start migration**. Monitor progress in the job list or dashboard.

Step 4 Deploy and verify Crosswork Data Gateways.

a) Log out and log in to the Crosswork UI at `https://<new_crosswork_ip>:30603`. Acknowledge the **Action to be taken** pop-up after redeploying Data Gateways.
b) Delete old Data Gateway VMs and install new gateways with identical IPs and names as previously recorded.
c) Verify that each Data Gateway is deployed and registered with Crosswork.
d) Check Data Gateway status in **Administration > Data Gateway Management > Virtual Machines**. Ensure **Operation** and **Administration** state are UP.
e) After all gateways are active, confirm pool migration at **Administration > Data Gateway Management > Pools** and that Data Gateways are automatically enrolled.
f) Log out and log back in again to Crosswork UI to trigger the **Action to be taken** pop-up, then click **Acknowledge** to complete migration.

   Do not use browser history links with a child path to access the UI; this prevents the pop-up from appearing.

g) If NSO is set to read-only mode, disable it.

Data and configuration are successfully migrated to the new Crosswork installation. Data Gateways are redeployed and operational in the target environment.

What to do next

- Verify all migrated services and Data Gateways are operational.
- Go to **Device Management** > **Network Devices** and ensure that all devices are reachable and all the nodes are active. Then, select **Actions**, and choose **Detailed sync all devices**.

  This initiates a synchronization of all devices, ensuring their configurations and operational status reflect the most recent migration.
- Perform any required post-migration configuration.

Orphaned SR-TE policies and RSVP-TE tunnels

An orphaned SR-TE policy or RSVP-TE tunnel is a network path instance that:

- is initiated by the PCE within Crosswork Network Controller after the most recent cluster data synchronization,
- is not included in the current HA data set, and
- cannot be modified through the user interface until properly synchronized.

Additional reference information

- Orphaned policies and tunnels may appear after a cluster HA switchover or a backup/restore operation.
- Crosswork Network Controller displays an alarm when orphaned TE policies or RSVP-TE tunnels are detected (**Alerts** > **Alarms and Events**).
- You can view details of orphaned policies/tunnels, but cannot modify them until they are properly synchronized.

How to manage orphaned policies and tunnels

Crosswork Network Controller provides APIs to help clear orphans. To list orphaned SR-TE policies or RSVP-TE tunnels, use the following:

- **cisco-crosswork-optimization-engine-sr-policy-operations:sr-datalist-oper** (for SR-TE policies)
- **cisco-crosswork-optimization-engine-rsvp-te-tunnel-operations:rsvp-te-datalist-oper** (for RSVP-TE tunnels)

Set **is-orphan=True** and use the GET action to retrieve the list. To make orphaned items manageable again, use the SAVE action for the corresponding policy or tunnel type.

Counter-examples

SR-TE policies or RSVP-TE tunnels that were synchronized before the last cluster data sync are not considered orphaned.

References

For more information, see API documentation on Devnet (**API Reference** > **Crosswork Optimization Engine**).

Crosswork Data Gateway disaster recovery scenarios

A disaster recovery scenario is a operational scenario that:

- addresses the re-establishment of Crosswork Data Gateway services after a system-wide disaster,
- involves steps that may vary depending on the number and types of Data Gateway VMs present, and
- determines whether additional manual procedures are required if Data Gateway VMs were deleted during the disaster.

Types of disaster recovery scenarios

- When all active and standby Data Gateway VMs in a pool have the **Operational state** set to **Error** after recovery. For recovery steps, see Restore Data Gateways after a disaster (with high availability), on page 22.
- When a pool contains only one Data Gateway VM, or multiple active Data Gateway VMs in the **Error** state without any standby VMs. For recovery steps, see Restore Data Gateways after a disaster (without high availability), on page 23.

Additional information

The disaster recovery process for Cisco Crosswork Network Controller automatically restores Data Gateway services in most cases. Manual procedures are only required if Data Gateway VMs have been deleted from the system during the disaster.

Restore Data Gateways after a disaster (with high availability)

Restore a Data Gateway pool with active and standby VMs after a disaster event, ensuring high availability and continued data collection.

Use this task after a disaster, when a Data Gateway pool with high availability is in the **Error** state and Cisco Crosswork disaster recovery is complete. This procedure returns the pool and devices to normal operation.

Before you begin

Before you begin:

- Complete the Cisco Crosswork disaster recovery operation.
- Ensure Crosswork data is restored and all pods are healthy and operational.
- Do not redeploy Data Gateways until Crosswork is fully restored.

Procedure

Step 1 Install new Data Gateway VMs using the same profile, hostname, and management interface as before the disaster.

The newly installed Data Gateway VMs will appear in the **Error** state because Crosswork restores data from the old VMs.

Step 2 Log in to Cisco Crosswork.

Step 3 Navigate to the **Administration > Data Gateway Management > Pools** page (or the equivalent for your environment).

Step 4 Select and edit the pool. Remove (unassign) the standby VM from the pool.

Step 5 Change the **Administration State** of the standby VM to **Maintenance** mode.

Note
If you redeploy the Data Gateway without first moving it to **Maintenance** mode, enrollment with Crosswork fails and errors appear in the logs. To resolve, switch to **Maintenance** mode or manually re-enroll the gateway.

Step 6 Edit the pool again and add the standby VM to the pool.

Adding the standby VM triggers a failover and the newly added VM becomes the active VM in the pool.

Step 7 Repeat steps 4–6 to restore the (now) standby VM that is still in the **Error** state.

Step 8 Verify the following:

- The pool has both an active and standby VM.
- Devices are attached to the active VM in the pool.
- Collection jobs are running as expected.

The Data Gateway pool is restored with high availability, and normal operation of devices and collection jobs resumes.

What to do next

- Monitor Data Gateway and device status to ensure continued normal operation.
- Address any remaining error states by reviewing logs or following troubleshooting procedures.

Related Topics

Change the Administration State of a Data Gateway, on page 74
Attach devices to a Data Gateway, on page 75
Detach devices from a Data Gateway, on page 77
Device assignment management, on page 73
Edit a Data Gateway pool, on page 71
Re-enroll Crosswork Data Gateway, on page 505

Restore Data Gateways after a disaster (without high availability)

Restore Data Gateway VMs and pools after a disaster in environments without high availability, so that device management and data collection can continue.

Use this task when you lose a Data Gateway VM during a disaster and your deployment does not use high availability. Choose the recovery option that fits your situation: replacing a VM, detaching or moving devices, or adding a standby VM. Each option restores device management and data collection capabilities.

Before you begin

Before you begin:

- Complete the Cisco Crosswork disaster recovery operation.
- Ensure all Data Gateway VM and pool information is restored and available in Cisco Crosswork.

Procedure

Step 1 Replace a lost Data Gateway VM with a new VM (same configuration as the original).

a) Log in to Cisco Crosswork and go to **Administration** > **Data Gateway Management** > **Data gateways**.
b) Delete the existing pool associated with the lost VM.
c) Set the Administration State of the VM to Maintenance.
d) Install a new Data Gateway VM with the same profile, hostname, and management interface as the lost VM.
e) Set the Administration State of the VM to Up.

The Operational State of the VM changes from Error to Not Ready.

f) Create a new pool with the same name as the original, and add the VM to this pool.

Verify the Data Gateway has Operational State as Up.

g) Attach devices to the Data Gateway as needed.
h) Verify that collection jobs are running as expected.

Step 2 Detach devices or move devices to another operational Data Gateway.

a) Log in to Cisco Crosswork and go to **Administration** > **Data Gateway Management** > **Data gateways**.
b) Detach devices from the affected VM or move devices to another Data Gateway that is Operational State Up.

c) Delete the existing pool. (Note: This action does not unassign the VM from the pool; it will still appear assigned.)
d) Set the Administration State of the VM to Maintenance.
e) Reboot the VM to unassign it from the pool.

After reboot, the VM enrolls with Cisco Crosswork automatically. Wait about 5 minutes, then verify the VM is administratively Up and in Not Ready state.

Note
You can also manually re-enroll the VM from the Interactive Console of the Data Gateway VM, if required.

f) Create a new pool with the same name and add the VM.
g) Verify Data Gateway has Operational State as Up.
h) Reattach devices or move devices back to this Data Gateway as needed.
i) Verify that collection jobs are running as expected.

Step 3 Add a standby VM to the pool (restore a pool with only one active VM or multiple VMs without standby).

Note
To restore multiple active VMs in a pool without standby VMs, repeat these steps for each active VM.

a) Install a new Data Gateway VM.
b) Log in to Cisco Crosswork and go to **Administration** > **Data Gateway Management** > **Pools**.
c) Add the new VM to the pool.

Adding a VM triggers a failover and the newly added VM becomes the active VM in the pool.

d) Edit the pool, remove the now-standby VM, and set its Administration State to Maintenance.

After about 5 minutes, the standby VM enrolls with Cisco Crosswork automatically and should be operationally Up and in Not Ready state.

Note
You can manually re-enroll the VM if necessary from the Interactive Console of the Data Gateway VM.

e) Add the standby VM back to the pool. Verify both active and standby VMs are operationally Up.
f) Verify the following:

- Devices are attached to the active VM in the pool.
- Collection jobs are running as expected.

Data Gateways and pools are restored, devices are reattached, and collection jobs resume as expected in a non-high availability deployment after a disaster.

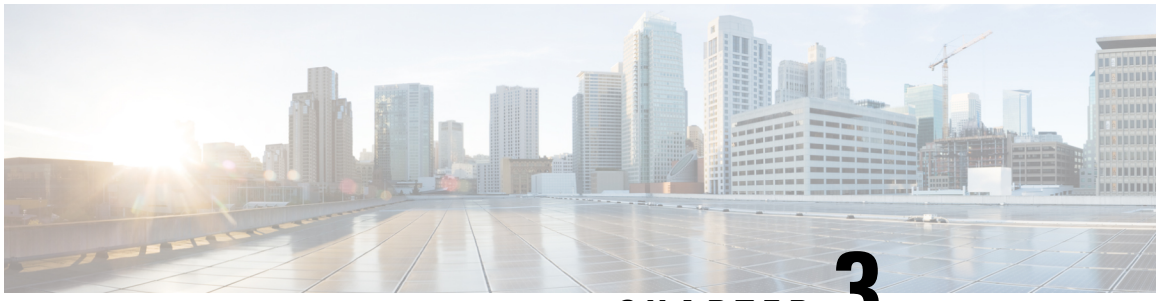
What to do next

- Monitor Data Gateway and collection job status to confirm normal operation.
- Review logs and troubleshoot if any VM remains in Error or Not Ready state.

Related Topics

Change the Administration State of a Data Gateway, on page 74
Attach devices to a Data Gateway, on page 75

Detach devices from a Data Gateway, on page 77
Device assignment management, on page 73
Edit a Data Gateway pool, on page 71
Re-enroll Crosswork Data Gateway, on page 505



CHAPTER 3

Manage the Crosswork Network Controller VMs

You can deploy Cisco Crosswork Network Controller on a single virtual machine or as a cluster of multiple VMs. This section covers essential concepts, tasks, and troubleshooting procedures for managing virtual machine nodes in any deployment scenario.

Virtual machines in Crosswork Network Controller

A virtual machine (VM) is a compute node that

- hosts platform services and applications,
- supports both standalone and clustered deployments, and
- enables administrators to monitor, configure, and scale system resources.

In this documentation, the terms **VM** and **node** refer to the same entity and are used interchangeably. Crosswork Network Controller supports two deployment models:

- **Single VM deployment**: All system functions run on a single virtual machine, providing a streamlined management experience with limited redundancy and device capacity.

- **Cluster deployment**: Multiple VMs form a cluster, distributing workloads for scalability, high availability, and extensibility.

Administrators use the Crosswork Manager interface to:

- monitor the health and status of each VM,
- view resource consumption and operational details,
- add, update, or remove VMs as network demands change, and
- assign administrative roles for VM management tasks.

Additional reference information

- Role assignment controls user access to VM configuration settings.
- Management actions and monitoring features are available for both individual VMs and clusters.
- For advanced operational guidance, see tasks such as deploying new VMs, troubleshooting faults, and performing system recovery.

Management actions in Crosswork Manager

The Crosswork Manager interface enables administrators to monitor and manage cluster health, resources, nodes, and installed applications.

Table 5: Crosswork manager actions

Action	Description
Navigation	Use the **Crosswork Manager** window to check the health of the cluster. To access: from the main menu, choose **Administration** > **Crosswork Manager**.
Crosswork summary tab	Displays summary information about the status of nodes, the Platform Infrastructure, and the applications currently installed.
Cluster Management window	Displays node details and can be viewed only when Crosswork Network Controller is deployed as a cluster. Click on the **System summary** tile to see the node details.
System Summary window	When deployed on a single VM, allows access to details for that VM. Click on the **System summary** tile to see the VM details.

Additional notes

- In a cluster, the Cluster Management window provides summarized details about cluster health, overall resource consumption, and per-node resource utilization.
- The UI shows the IP addresses in use for each node and whether they are hybrid or worker nodes.

- On AWS EC2 deployments, the VM status may show "unknown" initially and then "initializing" after updating the inventory file—this is normal behavior for EC2 clusters.
- To see more visualizations, use the **View more visualizations** link in the top-right corner.
- To inspect node details, click on a node tile and select **View details** for components, microservices, and alarms.
- To request metrics or logs, click  under the **Actions** column and select the desired operation (such as metrics, logs, or restart microservice).
- For additional platform or application health, refer to the **Crosswork health** tab.

Common troubleshooting scenarios in cluster management

These scenarios describe common troubleshooting cases in Crosswork Network Controller cluster management and their expected behaviors:

Table 6: Troubleshooting scenarios

Scenario	Resolution
One of the Hybrid nodes is faulty in a cluster with one or more worker nodes.	Follow the *Clean system reboot* procedure described in System recovery options and requirements, on page 45.
More than one Hybrid node is faulty.	Follow the *Redeploy and recover* procedure described in System recovery options and requirements, on page 45.
Last_updated_time deviation	On the **Cluster Management** window, it is normal to see deviation on the *last_updated_time* across the nodes in the cluster based on when the data was updated. This is an expected behavior.

Additional information

- If multiple node or application faults persist after recommended recovery actions, contact the Cisco Customer Experience team for further assistance.
- When performing recovery actions, always verify backup recency and ensure the operational architecture matches the original deployment (number/type of nodes).
- For further recovery steps, see System recovery options and requirements, on page 45 for detailed actions covering VM replacement, system reboot, and redeployment.

Edit data center credentials

Update and store the current credentials for your data center.

If you changed your password after deploying Crosswork Network Controller, update the stored credentials to ensure the correct password is used when deploying the new VM.

Before you begin

Ensure you have the current credentials for your data center.

Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager** .

Step 2 On the **Crosswork summary** tab, click the **System summary** tile to display the **Cluster Management** window.

Step 3 Choose **Actions** > **View/Edit data center** to display the **Edit data center** window.

The **Edit data center** window displays details of the data center.

Step 4 Use the **Edit data center** window to enter values for the **Access** fields: Address, Username, and Password.

Step 5 Click **Save** to save the data center credential changes.

The new credentials are saved for the data center and will be used for subsequent deployments.

Add a VM to the Crosswork Network Controller cluster

Add a new VM in Crosswork Network Controller cluster to expand your cluster and handle increased workload.

As your network grows and you add more Crosswork applications, you may need to expand resources to handle increased workload. You can add a new VM to your Crosswork Network Controller cluster to scale capacity. The deployment steps are similar whether you use the UI or the API; for API details, see Crosswork Network Controller APIs. This guide describes the procedure using the UI.

Important

- If you install your cluster manually, import the cluster inventory file into Crosswork Network Controller before deploying a new VM. The **Deploy VM** option remains disabled until you complete the import. For more information, see Import the inventory file, on page 31.
- When a new Worker (or Hybrid) node is added and an existing node is subsequently deleted, the system can become unstable and many pods may enter a degraded state. This occurs because the system requires a rebalance operation after the new node is added. To avoid instability, users must manually run the **Rebalance** option from the **Actions** tab immediately after adding the Worker/Hybrid node.
- If worker nodes are deployed on an ESXi host with a down Nexus connection, the nodes may appear as successfully added but will not join the cluster. Only nodes that successfully join (for example, hybrid nodes) are shown in the UI, while the backend may still reflect the total expected count. This behavior is expected because a node tile appears in the UI only after the VM boots and joins the cluster.

Before you begin

- Gather configuration details for Crosswork Network Controller, including the management IP address.
- Collect host information for the new VM, such as the data store and data VM interface IP address.
- Decide which type of VM to add. The cluster supports a minimum of three hybrid VMs and up to two worker VMs.

Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager**.

Step 2 On the **Crosswork summary** tab, click the **System summary** tile to display the **Cluster Management** window.

Note
The **Crosswork summary** tab and **Cluster Management** window both display the status of your cluster, but there may be slight differences. The **Crosswork summary** tab shows VM status based on Kubernetes, while the **Cluster Management** window also accounts for the VM status in the data center. For example, if a worker VM deployment fails due to insufficient data center resources, the **Cluster Management** window shows its status as *degraded*, while the **Crosswork summary** window shows the status as *down*.

Step 3 Select **Actions** > **Deploy VM** to display the **Deploy VM node** window.

Step 4 Enter the required VM details and configuration.

Step 5 Click **Deploy** to begin the provisioning process.

A new VM tile appears in Crosswork Manager and displays deployment progress.

Step 6 (Optional) To monitor deployment status, use **Cluster Management** > **Actions** > **View job history**, or check the data center UI.

Step 7 If needed, rebalance cluster resources or restart processes to optimize the load on the new VM. For more information, see Rebalance cluster resources, on page 36.

Import the inventory file

Import the Day0 inventory file to enable Crosswork Network Controller to perform any datacenter-related operations.

If you want to perform any datacenter-related operations, you must first manually import the Day0 inventory file.

Attention Crosswork Network Controller cannot deploy or remove VM nodes in your cluster until you complete this operation.

Before you begin

- Ensure you uncomment the `OP_Status` parameter in your tfvars file. Otherwise, VM status may display incorrectly as **Initializing** even after VMs become functional.
- n KVM or EC2 deployments (single VM or cluster), ensure that the tfvars file includes the required details for each VM in your setup and that the `NonVcenter` flag is set to `true`.

Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager** .

Step 2 On the **Crosswork summary** tab, click the **System summary** tile to display the **Cluster Management** window.

Step 3 Choose **Actions** > **Import inventory** to display the **Import Inventory** drawer window.

Step 4 (Optional) Click **Download sample template file** to download and edit the template. For more details on the installation parameters, see the *Installation Parameters* section in the *Crosswork Network Controller 7.2 Installation Guide* .

Step 5 Click **Browse** and select the cluster inventory file.

Step 6 Click **Import** to complete the operation.

The cluster inventory imports successfully, allowing Crosswork Network Controller to recognize and manage your VMs.

Export the inventory file

Export the Cisco Crosswork cluster inventory file for monitoring, management, or backup.

Use this process to download the current cluster inventory for external analysis, backup, or compliance.

Before you begin

Ensure you have administrator access to Crosswork Network Controller.

Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager** .

Step 2 On the **Crosswork summary** tab, click the **System summary** tile to display the **Cluster Management** window.

Step 3 Choose **Actions** > **Export inventory** .

Crosswork Network Controller downloads the cluster inventory gzip file to your local directory.

What to do next

Save or review the exported file as needed for your workflow.

Retry deployment for failed VMs

Retry deployment of nodes that failed due to incorrect information after correcting the details.

Node deployments with incorrect information can fail. After providing the correct details, you can retry the deployment.

Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager**.

Step 2 On the **Crosswork summary** tab, click the **System summary** tile to display the **Cluster Management** window.

Step 3 Click **Retry** on the failed node tile to display the **Deploy VM** window.

Step 4 Provide corrected information in the fields provided.

Step 5 Click **Deploy**.

Node removals

Node removals are cluster maintenance operations that

- allows administrators to delete failed or healthy nodes from a Cisco Crosswork cluster,
- eliminates the node reference from the Crosswork Network Controller cluster, and
- deletes the node from the host VM.

Node removal behaviors and limits

This topic lists the supported limits, expected effects, and actions associated with removing hybrid and worker nodes in the system.

Supported node roles and limits

- **Hybrid nodes**: The system must maintain three operational hybrid nodes at all times to ensure high availability (HA) and system protection. If one of the hybrid nodes stops functioning, Crosswork will attempt to compensate, but performance and resilience against further failures will be severely impacted. In such cases, the faulty node must be erased, and a new hybrid node should be deployed to replace it.
- **Worker nodes**: You can have up to two worker nodes. Both worker nodes can be erased without immediate consequences, but it is recommended to erase and replace them one at a time.

Effects of hybrid node removal

When a hybrid node is removed (either through an erase operation or directly from the backend), the following effects are observed:

- Remaining hybrid nodes display a "degraded" status, indicating high availability (HA) is lost.
- A further node failure could cause operational issues.
- Alarms are generated, and you are expected to restore the down node. Three functioning hybrid nodes should always be present.
- Several pods may enter the "Pending" state. This is expected because some critical infrastructure services, which run as three instances for maximum HA, are pinned to specific hybrid nodes.

- **Examples of services in the "Pending" state**: `cw-ftp`, `cw-sftp`, `nats`, `robot-etc`, `robot-kafka`, and `tyk`.

- Some pods may remain pending due to being configured as **DaemonSet**.
- Once the down hybrid node is restored, the system returns to normal and pending issues are resolved.

Effects of worker node removal

- Up to two worker nodes are supported.
- Both can be erased without immediate system impact.
- It is recommended to erase and replace worker nodes one at a time.

Note When a Worker node is removed while a vCenter alarm on that VM requires user acknowledgement, the node is deleted from the Crosswork Network Controller UI but not from the backend, causing the total count in the UI to remain incorrect and leaving the VM in vCenter. This stale backend entry can also cause new Worker node additions to fail with a duplicate-IP error. To clean up the stale entry, run this command:

```
robotctl remove-node-from-inventory <node-ip>
```

.

Manual cluster installation requirements

For manual cluster installations, you must erase the VM from the Crosswork UI and then delete it from the data center (for example, from vCenter).

Troubleshooting and escalation

If you continue to experience issues after performing these steps, contact the Cisco Customer Experience team for assistance.

Remove a node

Remove a node from Crosswork Network Controller.

Use this task to permanently erase a VM node in Crosswork Network Controller. This operation is disruptive and should be performed during a maintenance window.

Before you begin

- Erasing a node can disrupt services and block certain processes until the action completes. Perform this operation during a scheduled maintenance window.
- Removing worker or hybrid nodes increases the load on remaining nodes and may impact system performance. Contact Cisco Customer Experience before removing nodes.

Follow these steps to erase a node:

Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager** > **System summary**.

Step 2 On the VM node you want to remove, click and select **View details**.

Step 3 Click ··· and select **Erase VM node**.

Step 4 On the dialog prompt, click **Erase** to confirm the action.

Note

- During the removal of a hybrid or worker node, the Crosswork Network Controller UI may become temporarily unreachable for a short duration due to the relocation of the `robot-ui` pod to another node.
- A removed node will continue to be visible in the Grafana dashboard as an entry with only historical data.

The selected node is erased and removed from active management in Crosswork, but remains in Grafana as a historical entry.

What to do next

Review cluster performance and update operational procedures to account for the removed node.

Enable or disable maintenance mode

Use maintenance mode to temporarily suspend Crosswork Network Controller operations for maintenance or restart activities and resume normal service.

Maintenance mode provides a graceful shutdown for system updates and synchronizes application data before suspending services.

Attention It can take several minutes for the system to enter maintenance mode and to restart when maintenance mode is turned off. During these periods, users should not attempt to log in or use the Crosswork applications.

Before you begin

- Back up the Crosswork Network Controller cluster.
- Notify users, and ensure they log out. The operation cannot be canceled once started.

Procedure

Step 1 Navigate to **Administration** > **Settings** > **System Settings** > **Maintenance Mode**.

Step 2 To enable maintenance mode, set the **Maintenance mode** slider to **On**.

- When prompted, confirm the shutdown to proceed.
- Wait for the system to fully enter maintenance mode (this may take several minutes).

Note
If you plan to reboot the cluster, wait at least 5 minutes after entering maintenance mode to allow data synchronization.

Step 3 Perform required maintenance activities.

Step 4 To disable maintenance mode and resume service, set the **Maintenance mode** slider to **Off**.

When prompted, confirm the action. If you do not see a prompt but the system remains in maintenance mode, toggle it on and off again to restore applications.

Crosswork Network Controller enters or exits maintenance mode and synchronizes all application data. Users cannot access Crosswork applications during maintenance mode.

What to do next

Verify system state and notify users when service is restored.

Rebalance cluster resources

- Rebalancing ensures that workloads are evenly distributed, preventing performance bottlenecks caused by uneven resource utilization.
- Efficient resource utilization is critical for maintaining a healthy and well-performing cluster.

You can initiate rebalancing at any time through the user interface. Additionally, Crosswork Network Controller continuously monitors CPU usage across all VMs and will notify you if utilization exceeds predefined thresholds. These alarms serve as prompts to take corrective actions, such as adding more worker VMs and redistributing resources, before performance issues arise.

Rebalancing is required in these scenarios:

1. A new VM is added on day N in the cluster.
2. An existing VM is replaced on day N in the cluster.
3. A VM is down for over 5 minutes in the cluster.
4. The CPU or memory utilization of a VM constantly exceeds 95% in the cluster.

To avoid performance degradation, it is recommended to deploy new worker VMs (see Add a VM to the Crosswork Network Controller cluster, on page 30) before CPU usage exceeds 90%. However, note that when new VMs are added, active workloads are not automatically redistributed, making rebalancing a necessary step. If you already have 5 or 6 VMs in your cluster and still experience resource shortages, please reach out to the Cisco Customer Experience team for assistance.

Caution Rebalancing can take from 15 to 30 minutes during which the Crosswork Applications will be unavailable. Once initiated, a rebalance operation cannot be canceled.

To rebalance resources between the existing VMs in your cluster, follow these steps:

Before you begin

- Crosswork must be in maintenance mode before rebalancing to ensure data integrity.
- Any users logged in during the rebalancing will lose their sessions. Notify other users beforehand that you intend to put the system in maintenance mode for rebalancing, and give them time to log out. You can use the **Active Sessions** window (**Administration** > **Users and Roles** > **Active sessions** tab) to see who is currently logged in (or sessions that were abandoned and have not been cleaned up yet).

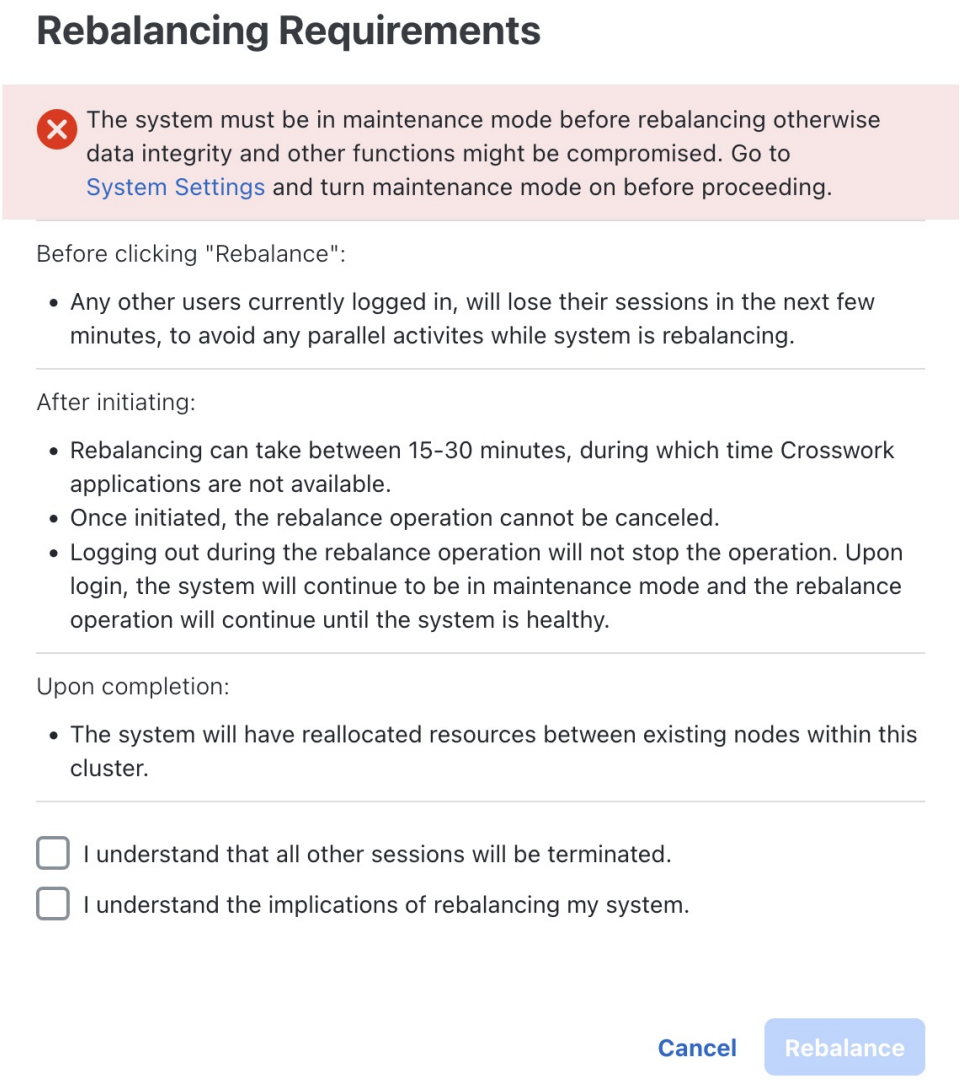
Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager**.

Step 2 On the **Crosswork summary** tab, click the **System summary** tile to display the **Cluster Management** window.

Step 3 Click **Actions** > **Rebalance**, and the **Rebalance Requirements** are displayed. Read through the requirements and select the two check boxes once you are ready to start the rebalancing.

Figure 1: Rebalancing requirements



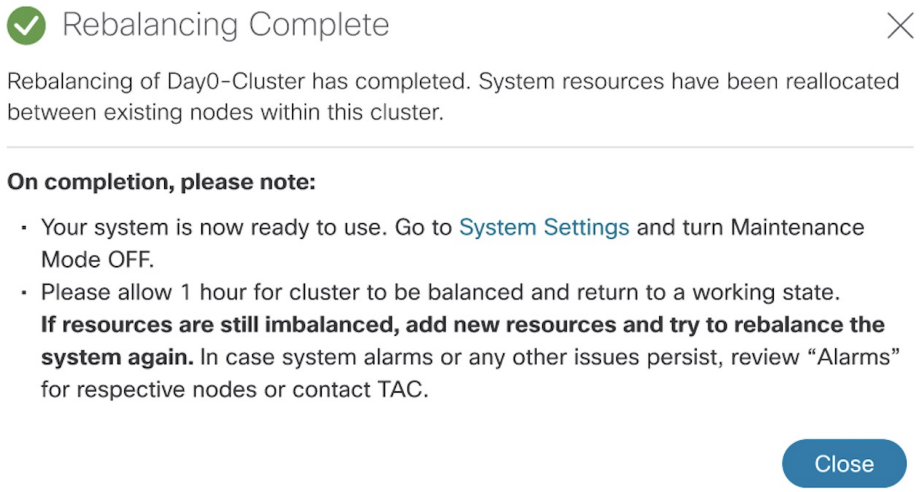
Step 4 Click **Rebalance** to initiate the process. Crosswork begins to reallocate the resources in the over utilized VM to the other VMs in the cluster.

A dialog box indicating the status of rebalancing is displayed. Kindly wait for the process to complete.

Step 5 After the rebalancing process is completed, you may see one of the following result scenarios:

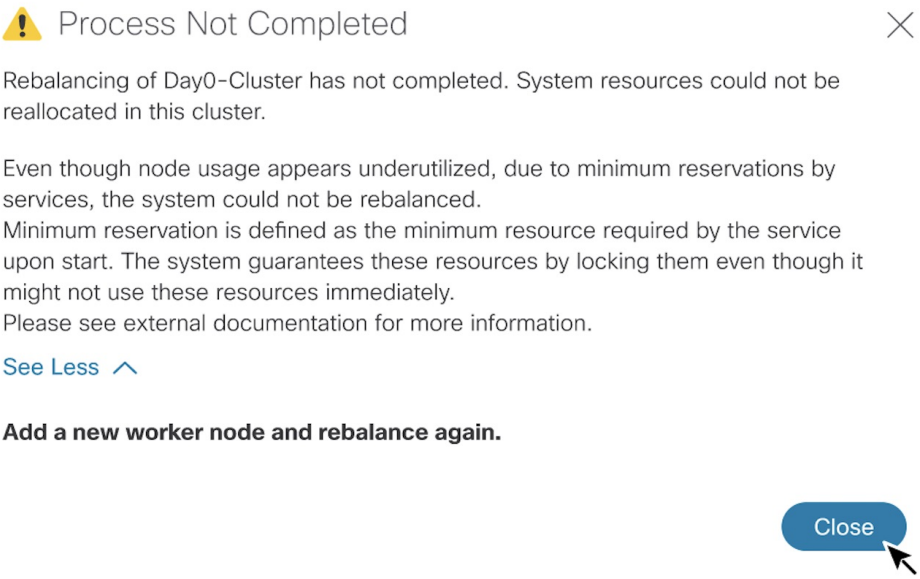
- **Success scenario:** A dialog box indicating successful rebalancing operation. Follow the instructions in the dialog box to proceed further.

Figure 2: Rebalancing result - success



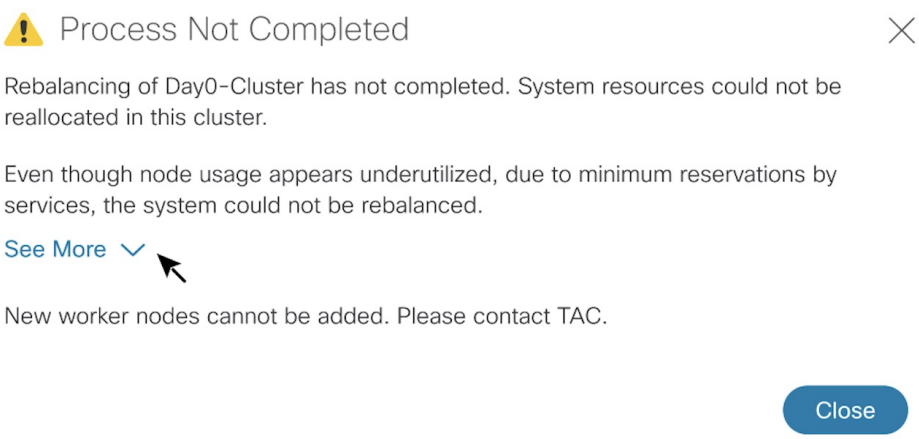
- **Failure scenario - scope available to add new worker nodes:** A dialog box indicating rebalancing failure is displayed. In this case, the system prompts you to add a new worker VM and try the rebalance process again.

Figure 3: Rebalancing result - add new worker node



- **Failure scenario - no scope to add new worker nodes:** A dialog box indicating rebalancing failure is displayed. In this case, the system prompts you to contact the TAC as new worker VMs cannot be added.

Figure 4: Rebalancing result - contact TAC



Best practice for moving workloads with placement APIs

Use these guidelines to ensure reliable workload movement in your cluster when using placement APIs, especially if the Crosswork Network Controller UI is unavailable or during VM or database recovery scenarios:

- The API method is preferred if the Crosswork Network Controller UI is not working due to high CPU utilization (>=95%) for a period of time.
- When replacing a VM containing a database, use the placement API to move the database before rebalancing workloads across the VMs.
- During a VM power-down and power-up scenario, typically the database pod recovers automatically within a few hours. If the VM is down for more than 5 minutes, redistribute resources using the placement API and rebalance the cluster.
- When moving non-core service and application workloads, exclude database services when identifying services to be moved.

Capabilities of placement APIs for workload distribution

Understand how placement APIs support manual workload movement between cluster VMs when automated or UI-based placement is unavailable.

You can use APIs to manually move database or application service workloads from one VM to other VMs in the cluster. The API method is preferred if the Crosswork Network Controller UI is not working due to high CPU utilization (>=95%) for a period of time.

Databases refer to `robot-postgres` and `cw-timeseries-db`. If a VM containing a database is replaced, the placement API must be explicitly invoked to instantiate the database on a new VM. In the event of VM replacement, the recommended order is to first use the API to move the database, followed by rebalancing to evenly distribute workloads across the VMs.

On clusters with worker VMs installed, the `robot-postgres` and `cw-timeseries-db` database services are pinned to the worker VMs, while the `local-postgres` pods are pinned to the hybrid VMs.

API example: place services for database pods

Request

```
curl --request POST --location
'https://<Vip>:30603/crosswork/platform/v2/placement/move_services_to_nodes' \
--header 'Content-Type: application/json' \
--header 'Authorization: <your-jwt-token>' \
--data '{
    "service_placements": [
        {
            "service": {
                "name": "robot-postgres",
                 "clean_data_folder": true,
                 "pin_to_node":true
            },
            "nodes": [
                {
                    "name": "fded-1bc1-fc3e-96d0-192-168-5-114-worker.cisco.com"
                },
                {
                    "name": "fded-1bc1-fc3e-96d0-192-168-5-115-worker.cisco.com"
                }
            ]
        },
        {
            "service": {
                "name": "cw-timeseries-db",
                 "clean_data_folder": true ,
                 "pin_to_node":true
             },
            "nodes": [
                {
                    "name": "fded-1bc1-fc3e-96d0-192-168-5-114-worker.cisco.com"
                },
                {
                    "name": "fded-1bc1-fc3e-96d0-192-168-5-115-worker.cisco.com"
                }
            ]
        }
    ]
}'
```

Response

```
{
    "job_id": "PJ5",
    "result": {
        "request_result": "ACCEPTED",
        "error": null
    }
}
```

API example: place services for non-core pods

Request

```
curl --request POST --location
'https://<Vip>:30603/crosswork/platform/v2/placement/move_services_to_nodes' \
--header 'Content-Type: application/json' \
--header 'Authorization: <your-jwt-token>' \
--data '{
    "service_placements": [
        {
            "service": {
                "name": "helios"

            },
            "nodes": [
                {
                    "name": "fded-1bc1-fc3e-96d0-192-168-5-114-worker.cisco.com"
                },
                {
                    "name": "fded-1bc1-fc3e-96d0-192-168-5-115-worker.cisco.com"
                }
            ]
        },
        {
            "service": {
                "name": "dg-manager"
             },
            "nodes": [
                {
                    "name": "fded-1bc1-fc3e-96d0-192-168-5-114-worker.cisco.com"
                },
                {
                    "name": "fded-1bc1-fc3e-96d0-192-168-5-115-worker.cisco.com"
                }
            ]
        }
    ]
}'
```

Response

```
{
    "job_id": "PJ5",
    "result": {
        "request_result": "ACCEPTED",
        "error": null
    }
}
```

Move services between cluster VMs using the placement API

Move database or application service workloads to different VMs in the cluster to address resource imbalances, high CPU utilization, or VM replacement events.

Perform this task when automated placement or the Crosswork Network Controller UI is unavailable, or during planned resource redistributions after VM replacement.

Before you begin

- Ensure you have your authorization token (`<your-jwt-token>`).
- Identify the names of services and target VMs (using Grafana or other cluster tools).
- Confirm access to the Grafana Monitoring Dashboard.

Follow these steps to move services between cluster VMs using the placement API:

Procedure

Step 1 Open the Grafana dashboard for the VM running the service using this link: *[Grafana Monitoring Dashboard](https://clusterendpoint:30603/grafana.monitoring/d/TYiQ9vgWk/platform-summary?orgId=1&refresh=1m\)*

Step 2 Identify the top five services with the highest CPU usage on the VM with the highest CPU utilization. Exclude database services by checking the pod CPU dashboard.

Step 3 Find the top three VMs with the lowest CPU utilization in Grafana.

Step 4 Use the placement API to move the top five services to the underutilized VMs.

For the required API request structure and examples, see Capabilities of placement APIs for workload distribution, on page 40.

Step 5 After moving services, monitor resource utilization in Grafana and follow the cluster rebalancing procedure as needed. For more information, see Rebalance cluster resources, on page 36.

Note
During a VM power-down and power-up, database replica recovery depends on the data size. Typically, the pod recovers on its own within a few hours. If the VM is down for more than 5 minutes in the cluster, redistribute the resources as described above and follow the cluster rebalancing procedure.

View job history

Use the **Job history** window to track the status of jobs, such as deploying a VM or importing cluster inventory.

Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager**.

Step 2 On the **Crosswork summary** tab, click the **System summary** tile to display the **Cluster Management** window.

Step 3 Choose **Actions** > **View job history**.

The **Job history** window displays a list of cluster jobs. You can filter or sort the **Jobs** list using the fields provided: Status, Job ID, VM ID, Action, and Users.

Step 4 Click any job to view it in the **Job details** panel at the right.

Tier upgrades

A tier upgrade is a process that:

- allows users to move from a lower tier to a higher tier in Crosswork Network Controller during the installation lifecycle,
- involves different procedures and requirements depending on whether the deployment is a cluster or a single VM, and
- supports ongoing scaling or feature expansion as business needs evolve.

For detailed information about available product tiers, see the *Release Notes for Crosswork Network Controller, Release 7.2.0*.

Note Ensure all operations are performed with minimal disruption to running workloads.

Upgrade the cluster tier

Follow these steps to upgrade Crosswork Network Controller on a cluster from a lower tier to a higher tier:

Procedure

Step 1 **Add new nodes** : Add new nodes to the cluster to accommodate more applications and resources required for the higher tier. For more information, see Add a VM to the Crosswork Network Controller cluster, on page 30

Step 2 **Move databases** : Move databases to worker nodes to optimize performance. For more information, see Capabilities of placement APIs for workload distribution, on page 40 .

Step 3 **Rebalance pods across nodes** : Use the rebalance feature to redistribute pods across new nodes and restore pod balance after any prolonged node shutdowns or power-ups. For more information, see Rebalance cluster resources, on page 36 .

Step 4 **Redeploy Data Gateway from Standard to Extended for higher tiers (Advantage, Premier)** : Put the Data Gateway in **Maintenance** mode by removing it from the pool and changing its role to **Unassigned** before redeploying. For more information, see Redeploy a Data Gateway VM, on page 79 and Change the administration state of a Data Gateway, on page 74 .

- **For protected pools** :
  a. Start the redeployment with the Data Gateway that has the role **Spare**, if the pool contains one, to minimize downtime for collections.
  b. Add the re-deployed Data Gateway back to the pool.
  c. Initiate a failover so the re-deployed Data Gateway becomes **Assigned** and resumes collections.
  d. Move the other Data Gateway (its role becomes **Spare** after the failover) out of the pool and redeploy it.
- **For unprotected pools** : Move the Data Gateways out of the pool and redeploy them. Collections may stop temporarily until the redeployment completes and the Data Gateways resume processing collection jobs.

Step 5 **Update the number of devices per Data Gateway based on tier** : Reduce the number of devices per Data Gateway as you move to a higher tier to align with the tier's requirements.

Upgrade the single VM tier

Follow these steps to upgrade Crosswork Network Controller on a single VM from a lower tier to a higher tier:

Procedure

Step 1 Create a backup of the current VM to secure all data. For more information, see Manage Backup and Restore, on page 9 .

Step 2 Deploy the higher tier build on a new VM. For installation instructions, see the *Install Cisco Crosswork Network Controller on a Single VM* chapter in *Crosswork Network Controller 7.2 Installation Guide* .

Step 3 Restore the data from the backup to the newly deployed VM.

Cluster system recovery

A cluster system recovery is a disaster recovery strategy that

- restores critical cluster services and data after failures or disruptions,
- addresses platform-specific considerations to ensure compatibility and resilience, and
- minimizes overall downtime to maintain business continuity.

A robust cluster system recovery approach helps ensure that Cisco Crosswork clusters can be restored quickly and reliably after failures, disruptions, or disasters. Understanding your recovery options and platform-specific requirements is essential to maintaining service continuity and minimizing downtime.

System recovery options and requirements

Successful cluster recovery depends on understanding platform requirements, backup practices, and the nature of the failure. This reference summarizes prerequisites, platform limitations, and actions for common recovery scenarios.

Before you begin

- For cluster recovery, it is essential to have a recent backup.
- The cluster you are restoring should have the same operational architecture, including the same number of hybrid and worker nodes.

Recovery conditions and system behavior

- At some time during normal operations of your Cisco Crosswork cluster, you may need to recover the entire system. This can result from malfunctioning nodes, services, applications, or a disaster destroying hosts for the cluster.

- A functional cluster requires a minimum of three hybrid nodes. These nodes share processing and traffic loads for management, orchestration, and infrastructure services.
- The hybrid nodes are highly available and can redistribute processing among themselves and to worker nodes automatically.
- The cluster can tolerate one hybrid node reboot (graceful or ungraceful); the system remains functional but with degraded availability.
- The system can tolerate any number of failed worker nodes (with degraded availability until restored).
- If two or more hybrid nodes are lost ("double fault"), recovery cannot be guaranteed – in such cases, redeploy a new cluster and restore from a recent backup.

Alarms and troubleshooting

- Cisco Crosswork generates alarms when nodes, applications, or services malfunction.
- Examine alarms and check health of the affected component(s). Use Crosswork features to drill down and, for service faults, attempt to restart the problem service.
- If alarms show a single hybrid node, or a hybrid plus worker node(s) failure, start by rebooting or replacing (erasing, then readding) failed nodes; if unsuccessful, attempt a clean system reboot.
- If the system remains unstable or degraded (loss of two or more hybrid nodes), deploy a new cluster and recover using a backup.

Platform limitations

- Unintentional VM shutdown is not supported on a 3 VM cluster running Crosswork Network Controller. If a VM fails, the remaining two VMs cannot support migrating all pods from the failed VM. Add worker nodes to enable VM shutdown.
- A reboot of one VM is supported in a 3 VM cluster. Restore may take 5 minutes (if the `orch pod` is not on the rebooted VM) up to 25 minutes (if it is).

Perform a clean system reboot (VMware)

Perform a coordinated reboot of all cluster VMs to restore operations or after failure.

A clean system reboot is sometimes required to restore cluster health following multiple node or service issues, or after system maintenance. This process ensures all VMs are properly powered down and brought back online in a specific order, supporting the stability and recovery of both hybrid and worker nodes in VMware deployments.

Follow these steps to perform a clean system reboot:

Procedure

Step 1 Place Crosswork Network Controller in Maintenance mode. See Enable or disable maintenance mode, on page 35 for details.

a) (Optional) Shut down Crosswork Data Gateways and other non-essential components, such as NSO and SR-PCE, that communicate with Crosswork.

Step 2 Power down all VMs:

a) Log in to the VMware vSphere Web Client.
b) In the **Navigator** pane, right-click the VM you want to shut down.
c) Choose **Power** > **Power Off**.
d) Wait for the VM's status to change to **Off**.
e) Repeat for each VM in the cluster.

Step 3 Power up the VM hosting the first hybrid node:

a) In the **Navigator** pane, right-click the VM to power up.
b) Choose **Power** > **Power On**.
c) Wait for the VM's status to change to **On**, then wait 30 seconds before continuing.

Step 4 Repeat the previous step for each remaining hybrid node, staggering reboots by 30 seconds. Continue with each worker node using the same staggered interval.

Step 5 After all VMs are powered on, wait a few minutes and login to Crosswork Network Controller.

Step 6 Move Crosswork Network Controller out of maintenance mode. See Enable or disable maintenance mode, on page 35 for details.

- If your cluster is not healthy, maintenance mode attempts may fail. Alarms may indicate failed services and reasons.
- If issues persist, follow the "redeploy and restore" method. For more details, see Redeploy and restore a Crosswork cluster from backup (VMware), on page 47.

Step 7 Restart Crosswork Data Gateways and any other components in your ecosystem that communicate with Crosswork Network Controller.

The Crosswork Network Controller cluster completes a clean system reboot. If cluster health does not return, proceed with the redeploy and restore procedure.

Redeploy and restore a Crosswork cluster from backup (VMware)

Rebuild and restore a failed Crosswork cluster using a previously taken backup.

Redeployment and restoration from backup is required when a cluster is severely degraded (such as after double faults or catastrophic failures), and cannot be recovered through standard node replacement or reboot procedures. The procedure involves powering down and deleting existing VMs, deploying a new cluster, and then restoring system state from a backup to recover services and data.

Before you begin

- Ensure you have a recent and valid backup file.
- This method assumes you have taken periodic backups before recovery is required. (For details on backup, see Back up data, on page 12.

Follow these steps to redeploy and restore the cluster:

Procedure

Step 1 Power down all VMs:

a) Log in to the VMware vSphere Web Client.
b) In the **Navigator** pane, right-click the VM you want to shut down.
c) Choose **Power** > **Power Off**.
d) Wait for the VM's status to change to **Off**.
e) Repeat for each VM in the cluster.

Step 2 Delete all VMs:

a) In the VMware vSphere Web Client **Navigator** pane, right-click the VM you want to delete.
b) Choose **Delete from Disk**.
c) Wait for the VM's status to show **Deleted**.
d) Repeat for each VM in the cluster.

Step 3 Deploy a new Cisco Crosswork cluster as explained in the *Cisco Crosswork Network Controller 7.2 Installation Guide*.

Step 4 Recover the system state to the newly deployed cluster. For more information, see Restore data after a disaster, on page 14.

A new Crosswork Network Controller cluster is deployed, and system state is restored using the most recent backup.

Shut down and restart the standby cluster safely

Safely shut down the standby cluster without Maintenance Mode and bring it back online with data consistency.

In geo HA deployments, the standby cluster can be shut down while data continues syncing from the active cluster, ensuring consistency without the need for Maintenance Mode.

Before you begin

- Ensure you do not place the standby cluster in Maintenance Mode.
- Verify that data is syncing from the active cluster.

Follow these steps to shut down and restart the standby cluster safely:

Procedure

Step 1 Shut down the standby cluster without placing it in Maintenance Mode.

Step 2 Keep the active cluster running so it continues syncing data during the shutdown.

Step 3 Power on the standby cluster when needed to start its automatic recovery.

Step 4 Wait for the standby cluster to become fully healthy, which may take about 20–40 minutes.

Step 5 Trigger an on-demand sync from the active cluster or wait for the next periodic sync.

The standby cluster returns to a fully healthy state with all data synchronized from the active cluster.

Collect cluster logs and metrics

Monitor or audit Cisco Crosswork cluster components by collecting and managing periodic logs and metrics for each cluster component.

Collecting logs and metrics helps administrators track the health and performance of the Cisco Crosswork cluster, including its nodes and microservices. Use this task for troubleshooting or routine audits.

Note Showtech logs must be collected separately for each application.

Before you begin

- Ensure you have administrator access to Cisco Crosswork Manager.
- Know which components (cluster, node, or microservice) you want to collect logs or metrics from.

Procedure

Step 1 From the main menu, select **Administration** > **Crosswork Manager**.

Step 2 On the **Crosswork summary** tab, select **System summary** to open cluster management.

Step 3 To collect logs and metrics for the entire cluster, click **Actions** and choose a showtech option:

- **Request all**: Collect both logs and metrics.
- **Request metrics**: Collect only metrics.
- **Collect logs**: Collect only logs.

Step 4 To collect logs or metrics for a specific node:

a) Select the node.
b) Click **Showtech options** and choose a showtech operation.

Step 5 To collect logs or metrics for an individual microservice on a node:

a) Under **Actions** for the desired microservice, click and select a showtech operation.

Step 6 To view the status of showtech jobs, select **Actions** > **View showtech jobs**. Under the **Action** column, use menu to:

- **Publish** a completed showtech log.
- **Delete** a showtech log.

- **View details** of a job.

The system collects and displays the requested logs and metrics for your chosen cluster component. Collected showtech logs are available for audit, troubleshooting, or compliance verification.

What to do next

Review collected logs and metrics as needed, and publish or delete showtech logs to manage storage or share information with other stakeholders.

Crosswork Network Controller containers

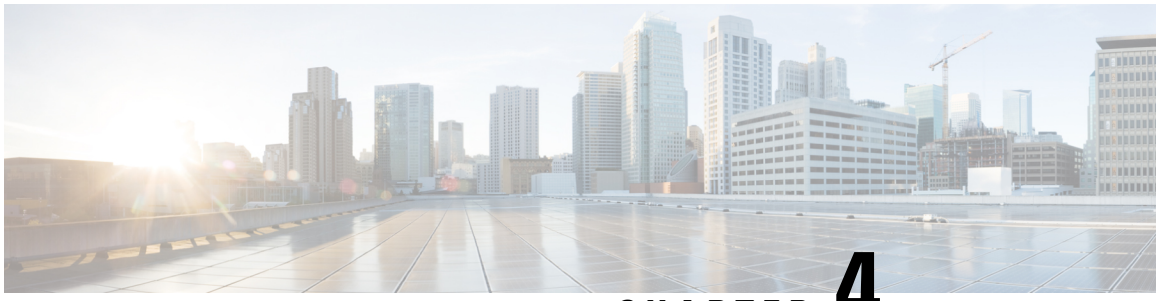
To give users a single reference that explains what each container does at a basic level, helping them identify components quickly when collecting logs or investigating issues.

Attention This topic includes information only for the containers that were available at the time of publication. It does not represent a complete list of all system containers.

Table 7: Crosswork Network Controller containers

Container name	Container role
robot-ui	This container provides the user interface. In a clustered environment, multiple instances run for resiliency. It typically starts after the core services are up, ensuring that all required processes are available before users can log in.
robot-dlminvmgr	The device lifecycle manager (dlm) tracks devices as they are onboarded to Crosswork Network Controller and monitors their health through basic reach checks.
robot-kafka	Kafka is an open-source messaging system used by Crosswork Network Controller services to process large volumes of streaming data.
nats	The nats is a lightweight, open-source messaging system used by Crosswork Network Controller services.
robot-etcd	The etcd is an open source key value database used by services on Crosswork Network Controller.
descheduler	The descheduler runs on demand and is responsible for moving services to help balance container placement and optimize resource usage across the nodes.
robot-orch	The orchestrator manages infrastructure services, including application lifecycle operations, backup and restore, geo HA functions, node management, and cluster management.

Container name	Container role
docker-registry	This component is part of the Crosswork Network Controller application lifecycle and handles installing and uninstalling Crosswork Network Controller applications within the cluster, servicing Kubernetes requests for Docker images.
cw-sftp	This component provides an SFTP server for applications that need to download device-related files during the application lifecycle.
cw-ftp	This component provides an FTP server for applications that need to download device-related files during the application lifecycle.
cw-ipsec	This component encrypts pod-to-pod communication across nodes.



CHAPTER 4

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.

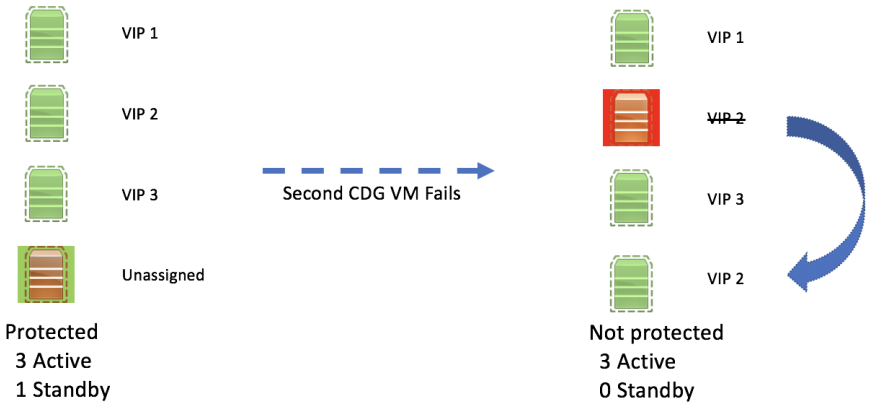
A Data Gateway pool can be in one of several states:

- 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 5: 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 56.
- 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 57.

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.

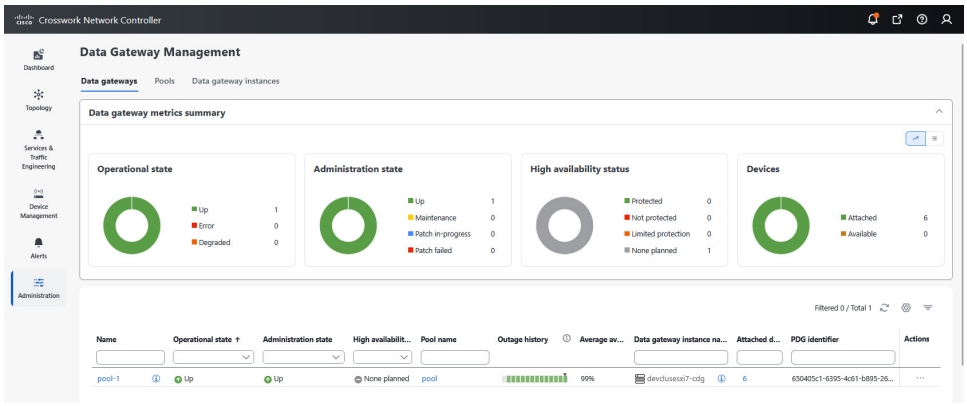
Procedure

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 6: Data Gateway management



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 8: 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 75. • Detach devices. For more information, see Detach devices from Data Gateway, on page 77. • Move devices. For more information, see Move devices to a different Data Gateway, on page 76. • Initiate a failover. For more information, see Perform a manual failover, on page 72.

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 63.
   - (Optional) Create the Data Gateway pools in geo-redundancy sites. See Create a pool in the geo redundancy-enabled sites, on page 67.
   - Attach devices to the Data Gateway. See Attach devices to Data Gateway, on page 75.
   - Verify that the default collection jobs are created and are running successfully. See Monitor the collection jobs, on page 117.
2. Extending Data Gateway capabilities (Optional).

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

Table 9: 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 104
Forward data to external data destinations.	External data destinations, on page 91
Create custom collection jobs that function independently from those built by Cisco Crosswork.	Create a collection job from Crosswork UI , on page 111

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 63
- Create a pool in the geo redundancy-enabled sites, on page 67
- Assign Data Gateways to geo redundancy-enabled sites, on page 70
- Edit or delete a Data Gateway pool, on page 71

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.

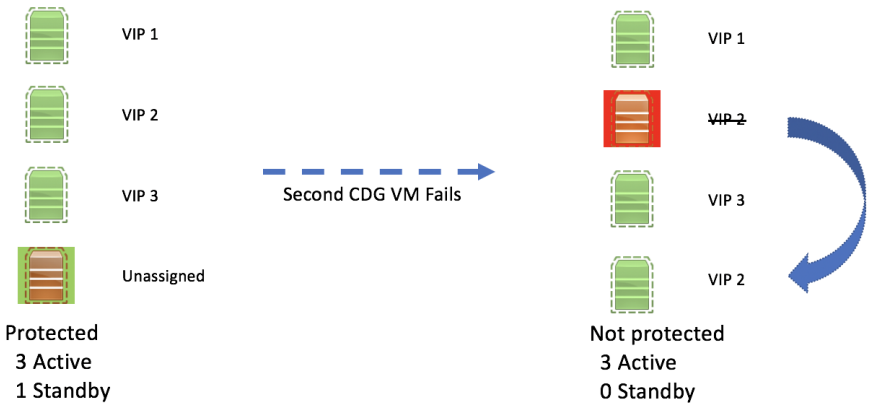
A Data Gateway pool can be in one of several states:

- 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 7: 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 65.

Complete these steps to create a Data Gateway pool.

Procedure

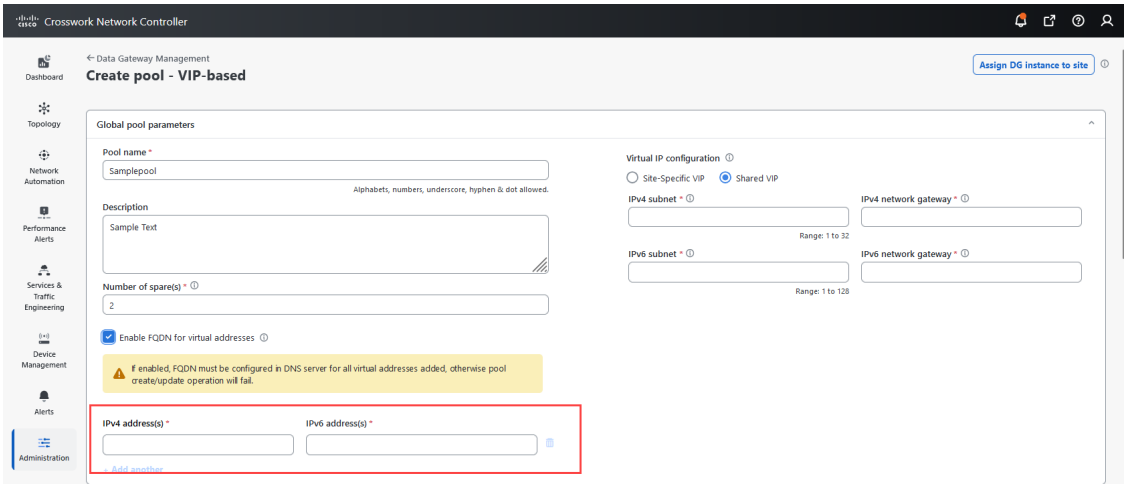
Step 1 Navigate to the **Administration** > **Data Gateway Management** > **Pools** tab.

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 66.

Figure 8: VIP-based pool for single stack deployment



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

Figure 9: VIP-based pool for dual-stack deployment

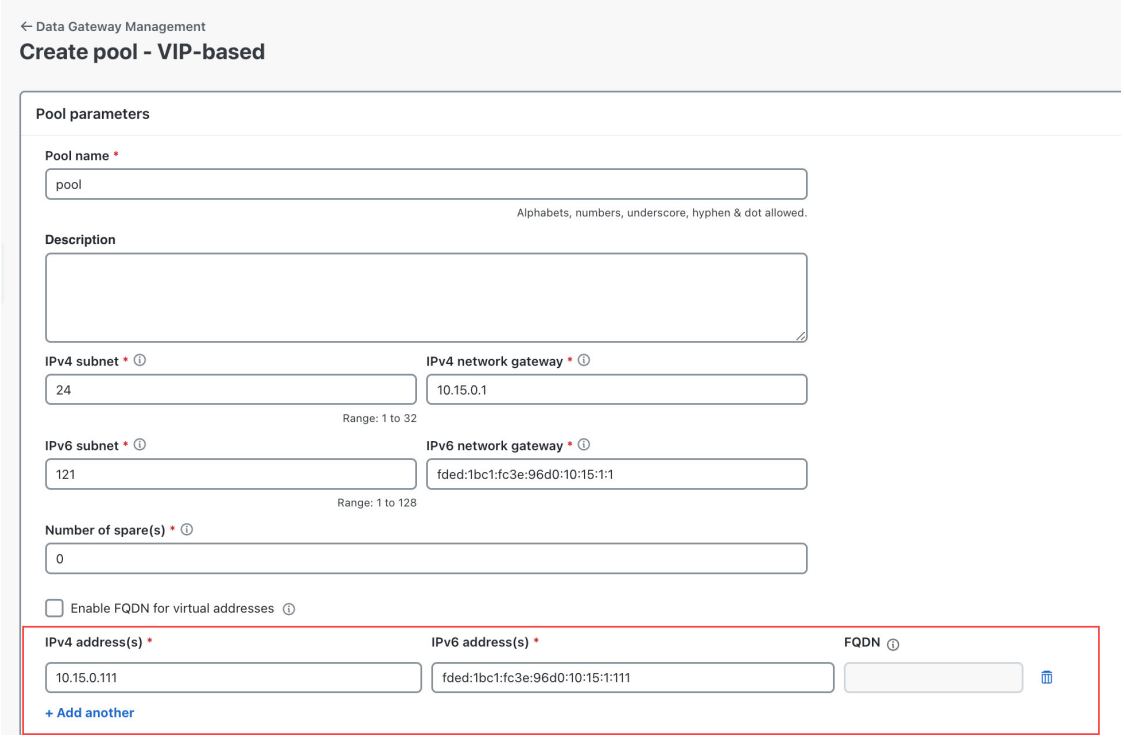
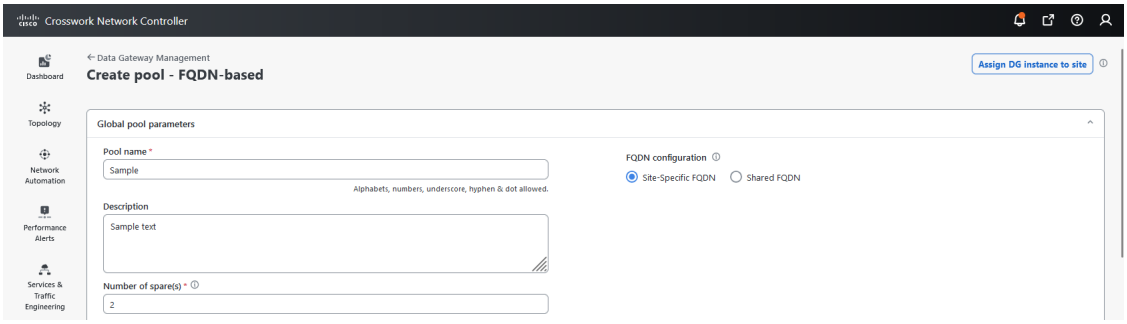


Figure 10: FQDN-based pool



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 10: 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 65.

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 66.

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 11: VIP-based pool

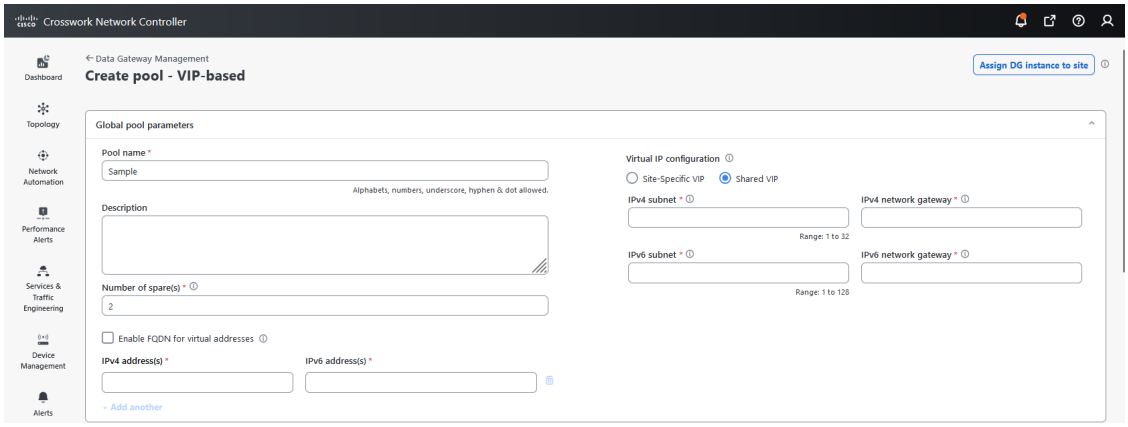
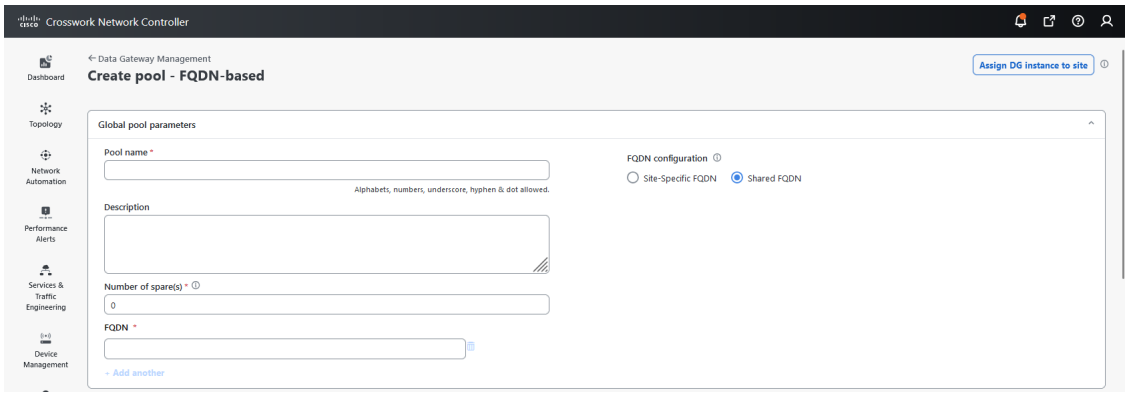


Figure 12: FQDN-based pool



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 13: Active pane for single stack

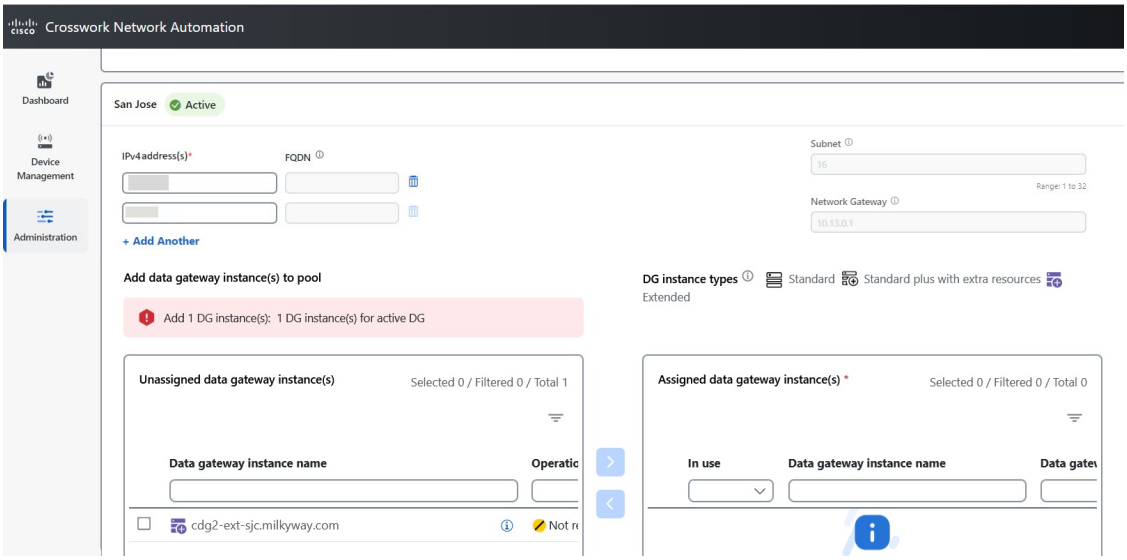
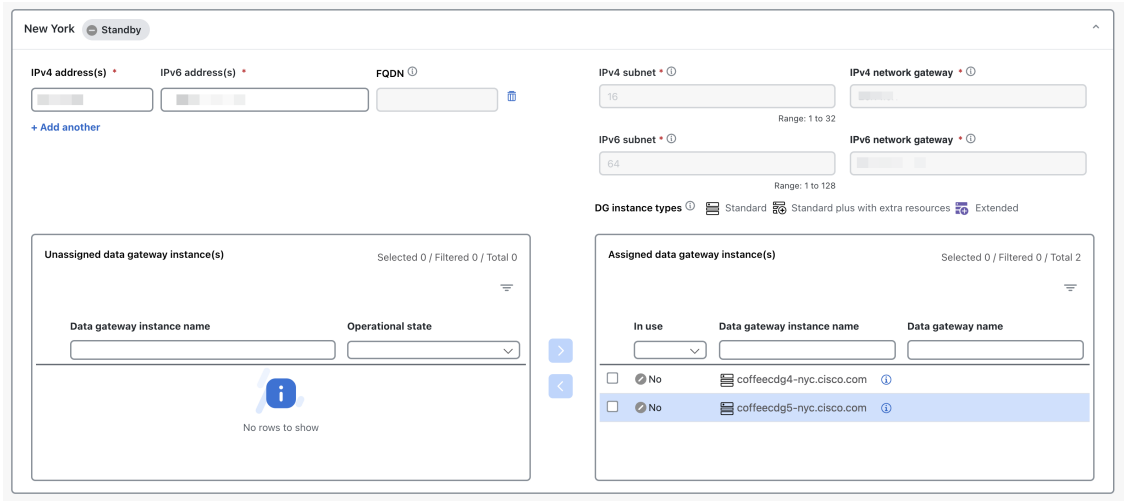


Figure 14: Active pane for dual stack



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 72.

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 163.

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

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 57

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.

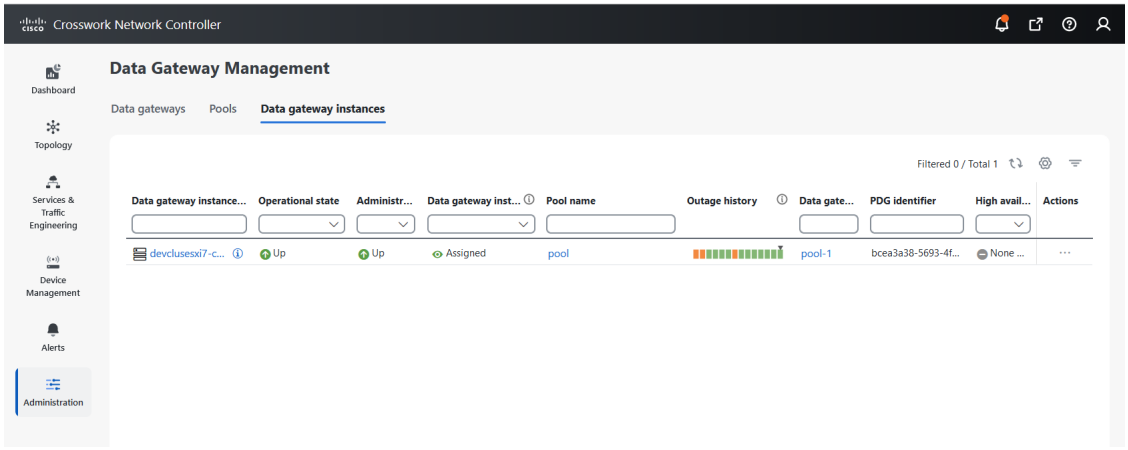
Procedure

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 15: Data gateway instances



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

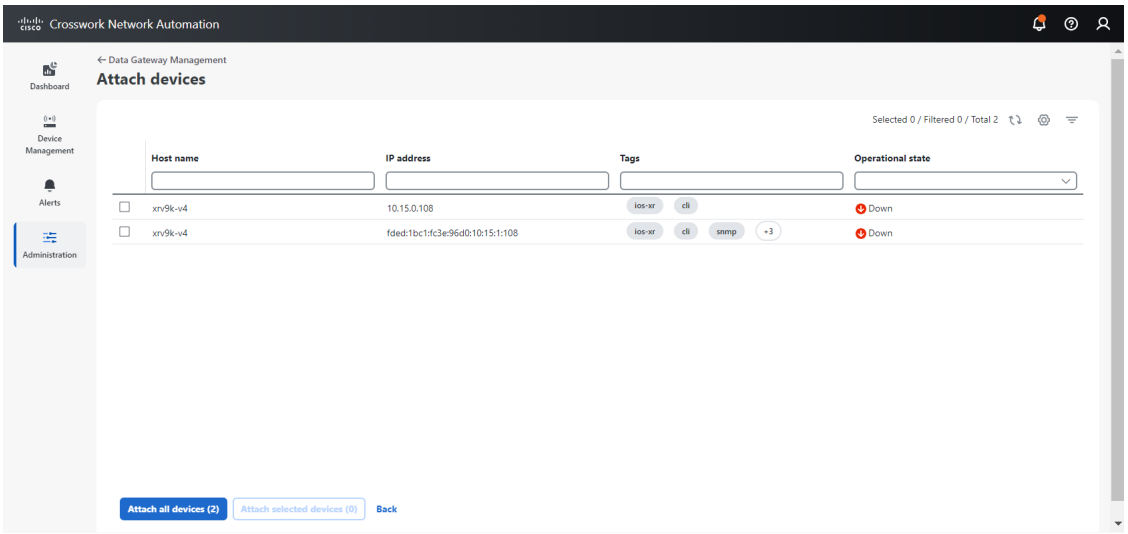
Verify that you are familiar with the prequsites to successfully attach the devices to the Data Gateway. For more information, see Requirement: Device assignment prerequisites.

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 16: Attach devices



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

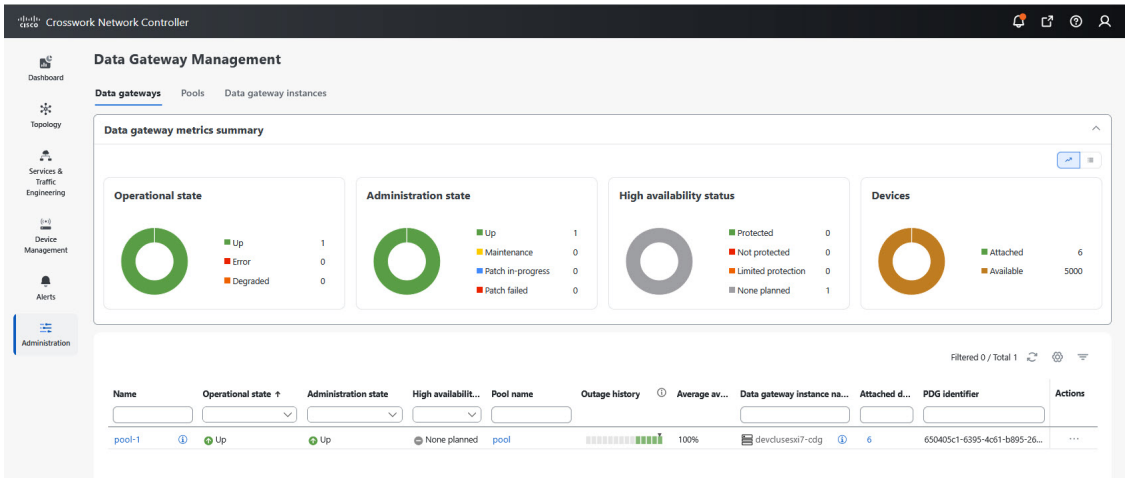
Before you begin

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 17: Data gateways



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

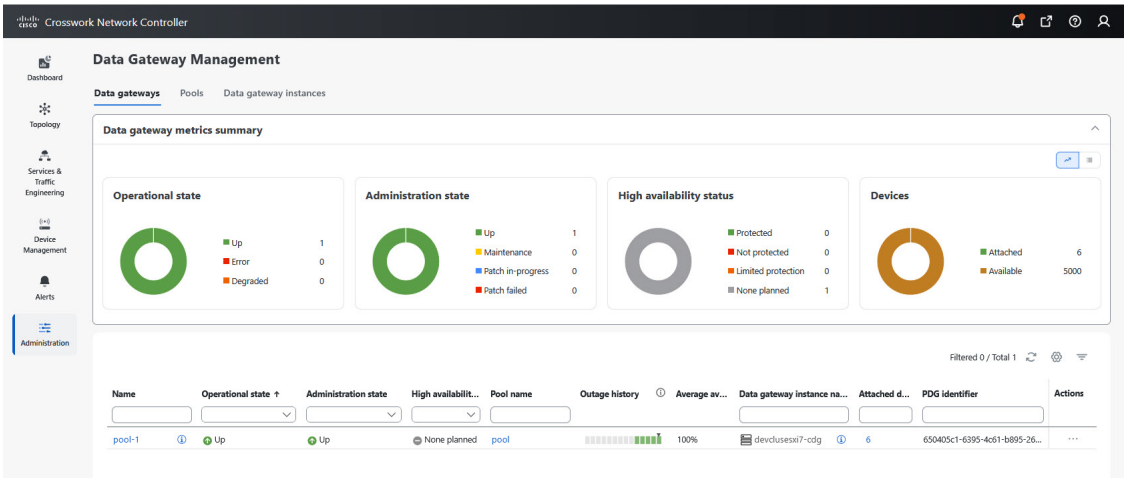
Before you begin

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**.

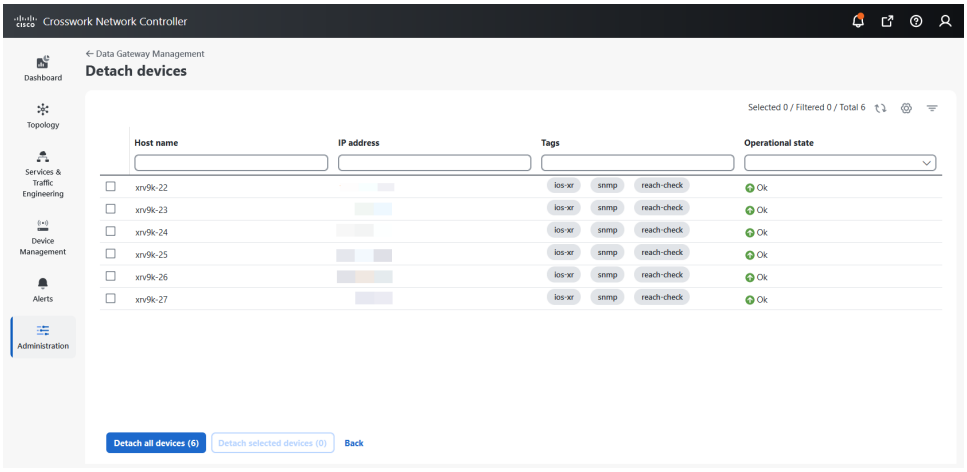
Figure 18: Data gateways



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 19: Detach devices



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 72.

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.

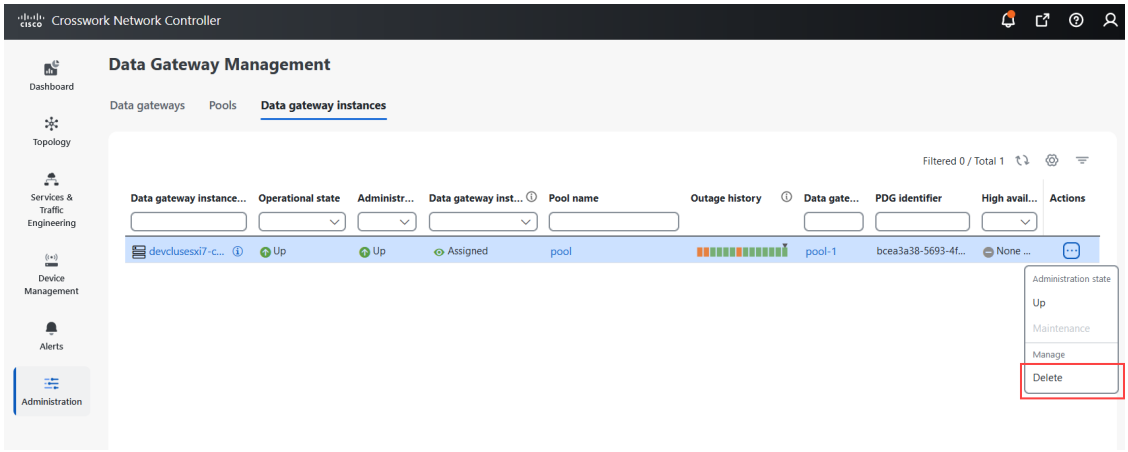
Use these steps to delete the Data Gateway instance from Crosswork Network Controller.

Procedure

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

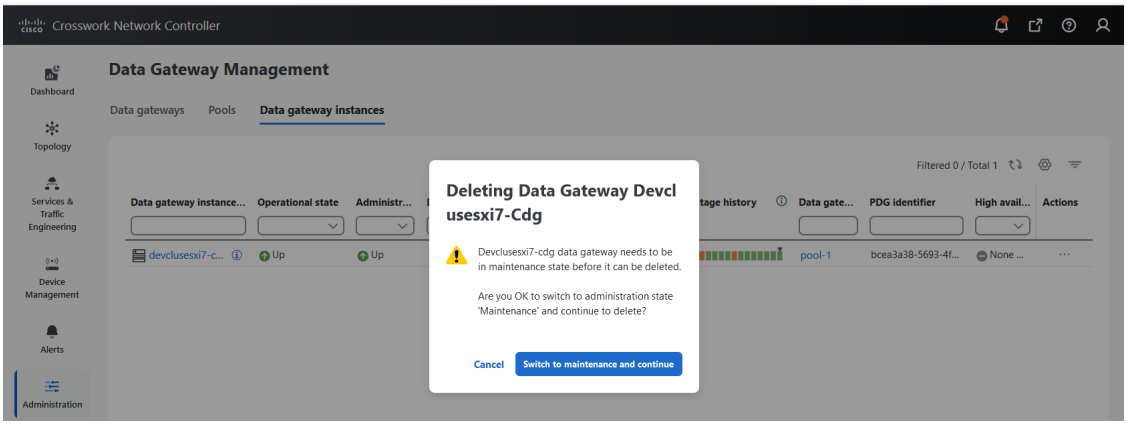
Step 2 Select the Data Gateway instance you want to delete, click **Delete** under **Actions**.

Figure 20: Data Gateway instances



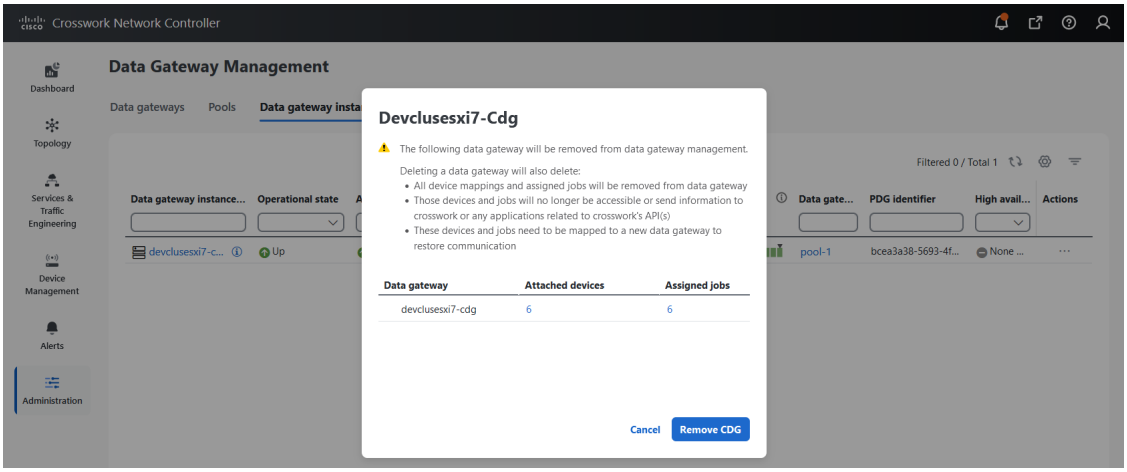
Step 3 If prompted, switch the Data Gateway instance to maintenance mode by clicking **Switch to maintenance & continue**.

Figure 21: Switch to maintenance mode confirmation message



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

Figure 22: Delete Data Gateway confirmation message



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 82
- Download the showtech logs, on page 157
- Download service metrics, on page 85
- Reboot Data Gateway VM, on page 86

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).

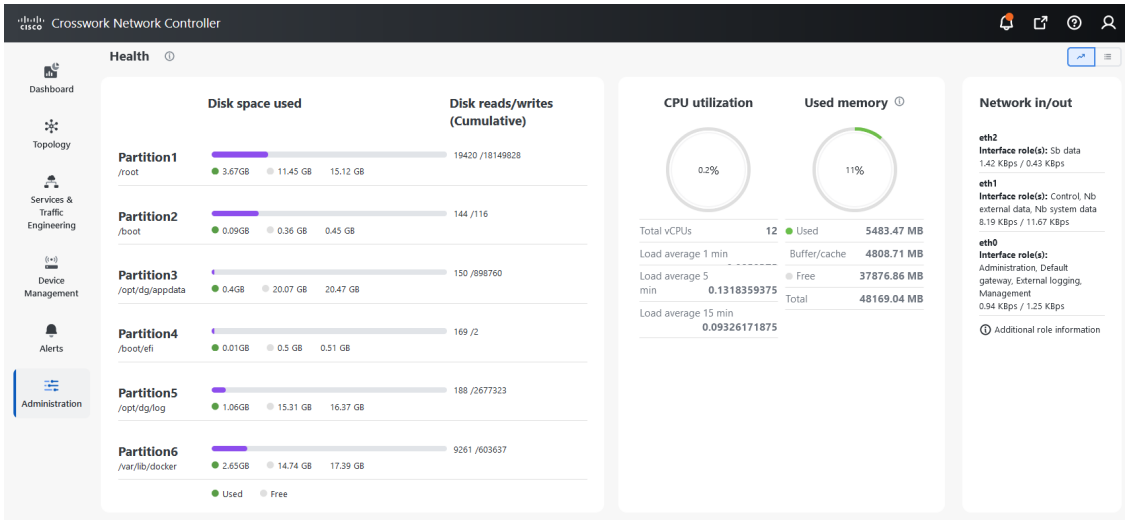
Key metrics and diagnostic tools

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 23: Crosswork Data Gateway health



- 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.

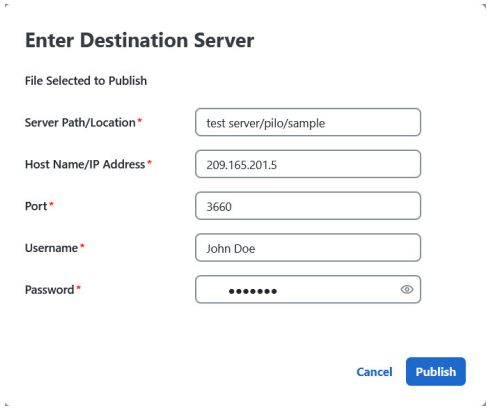
Step 3 In the Microservices tab, filter by "alarms" to locate the alarm pod.

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 24: Edit destination servers



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.

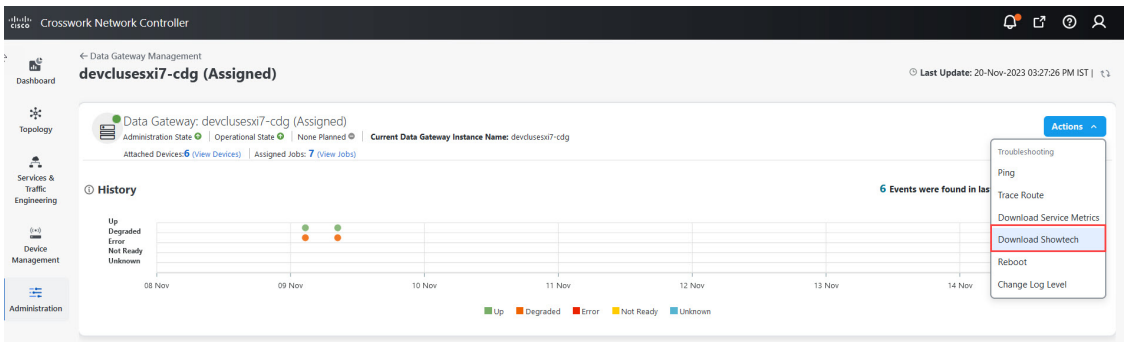
Procedure

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**.

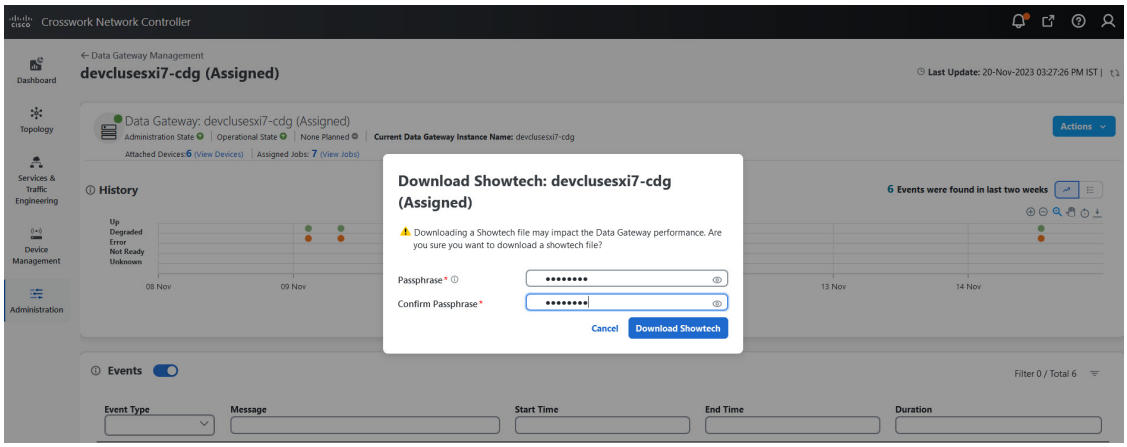
Figure 25: Download showtech



Step 4 Enter the desired passphrase.

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

Figure 26: Download Showtech pop-up



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.

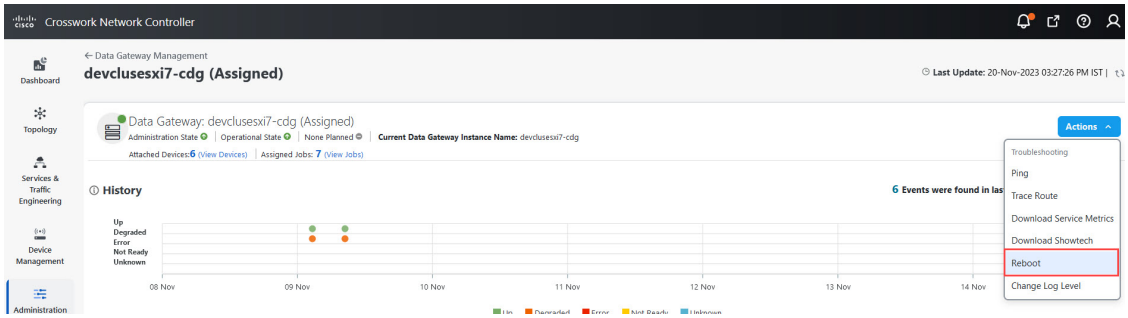
Procedure

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

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

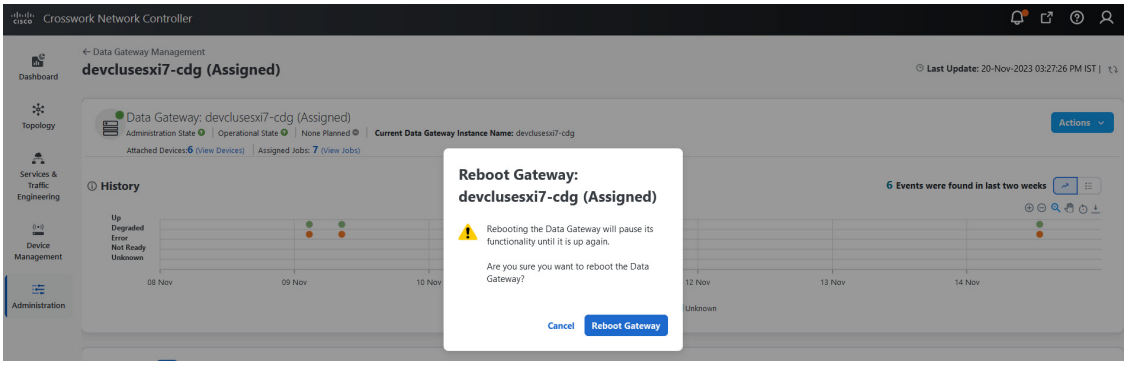
Step 3 On the **Crosswork Data Gateway details** page, at the top-right, click **Actions**, then click **Reboot**.

Figure 27: Data Gateway reboot



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

Figure 28: Reboot Data Gateway pop-up



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 87
- Allocate the Data Gateway resources , on page 89
- Enable or disable collectors, on page 90

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 88.
- Confirm that you are aware of the guidelines to update the ports. See Guidelines for updating port values, on page 88.

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 88.

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 88.

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 11: 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

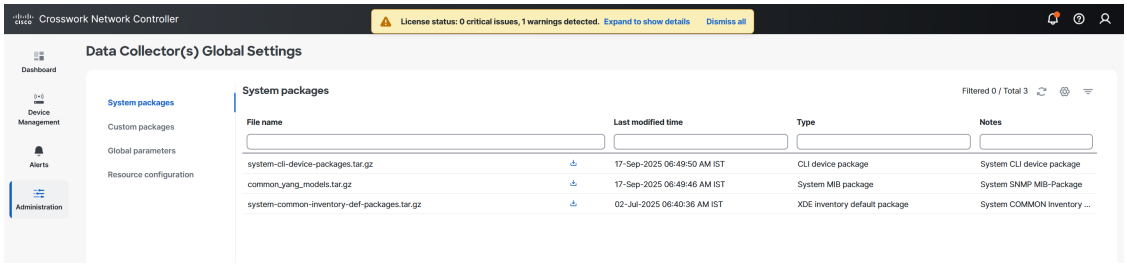
Ensure that you are aware of these points.

- 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 29: Resource configuration***



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 89.

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.

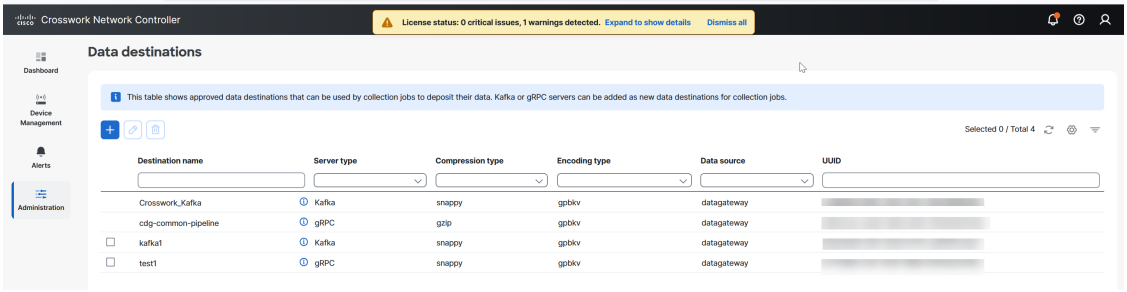
The **Data destinations** page allows users to:

- 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 30: Data destinations



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 96.

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**.

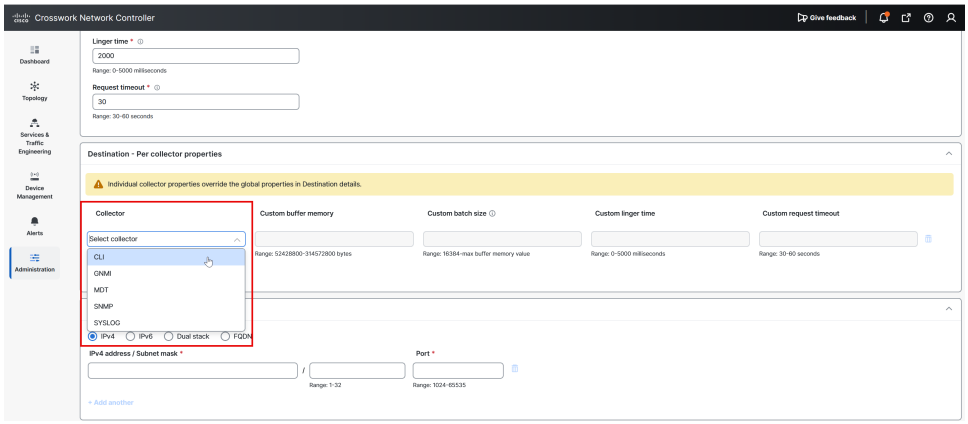
b) Enter the values as:

- **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 31: Add destination



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 96.

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 96.

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 12: 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 13: 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:

- `destinationTypee`
- `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 106. Then, follow the procedure to upload the custom device packages. See Upload custom packages, on page 108.

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 106.

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.

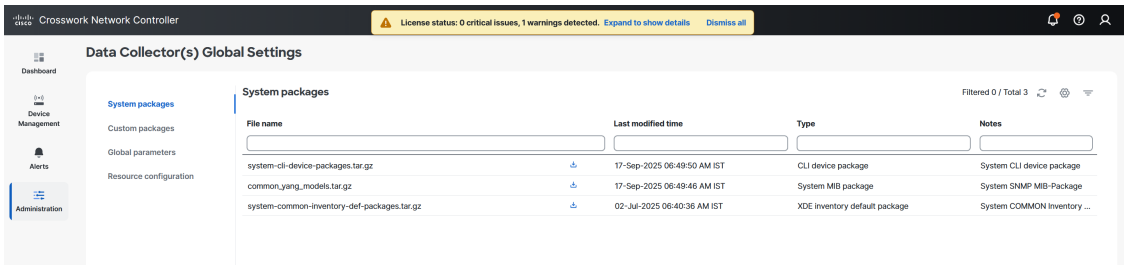
Downloading a device package

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 32: System device packages



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 91.
  - 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 111.
- 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 116.
- 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.

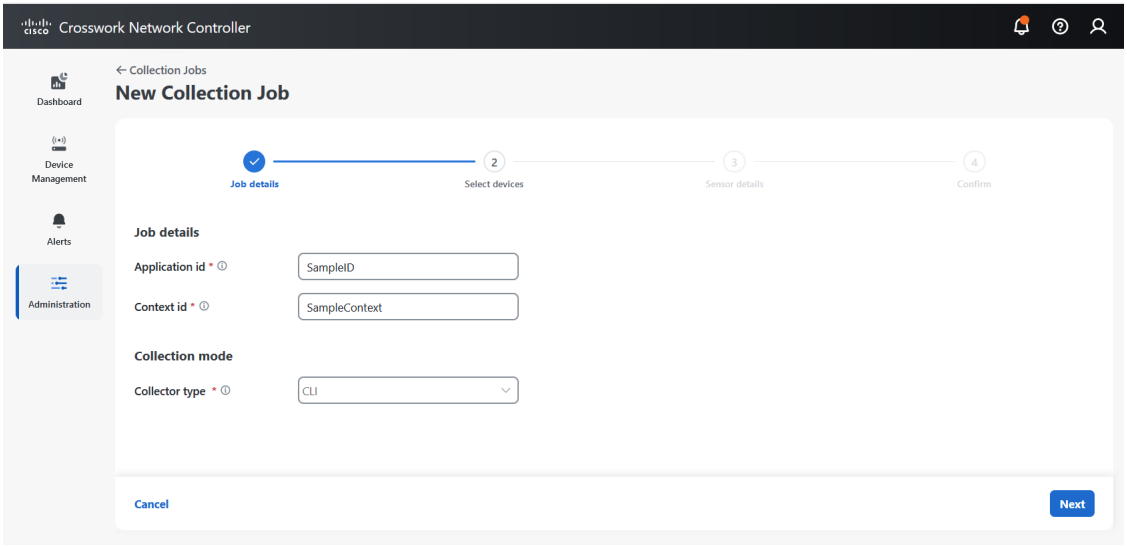
Procedure

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 33: New collection



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

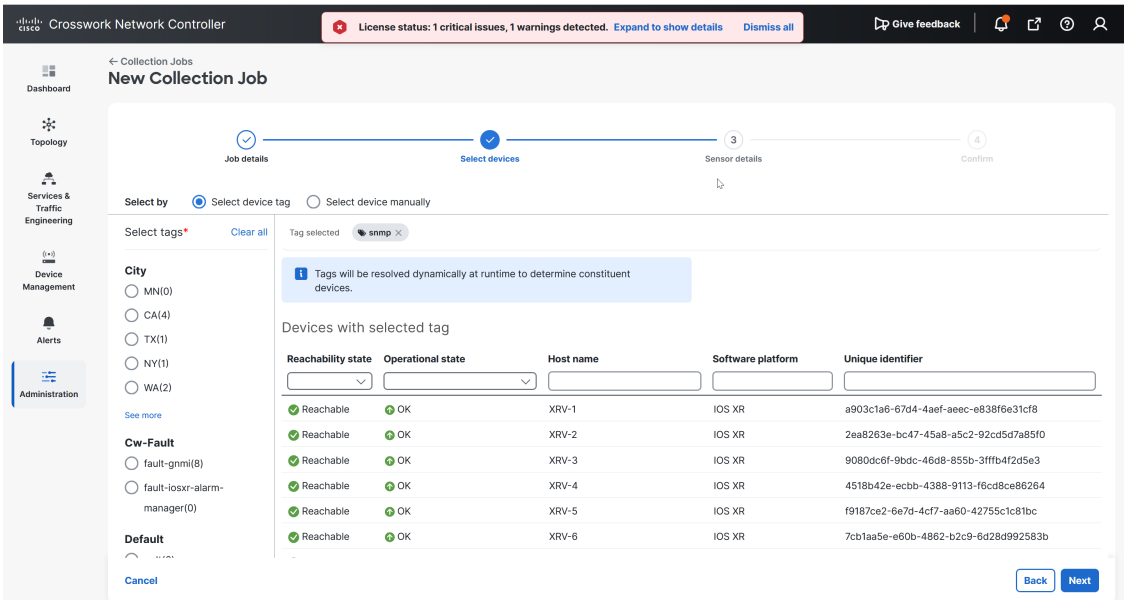
b. **Context Id**: Enter a unique identifier for your application subscription across all collection jobs.

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 34: Select devices



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 116.

Figure 35: Sensor details for CLI path

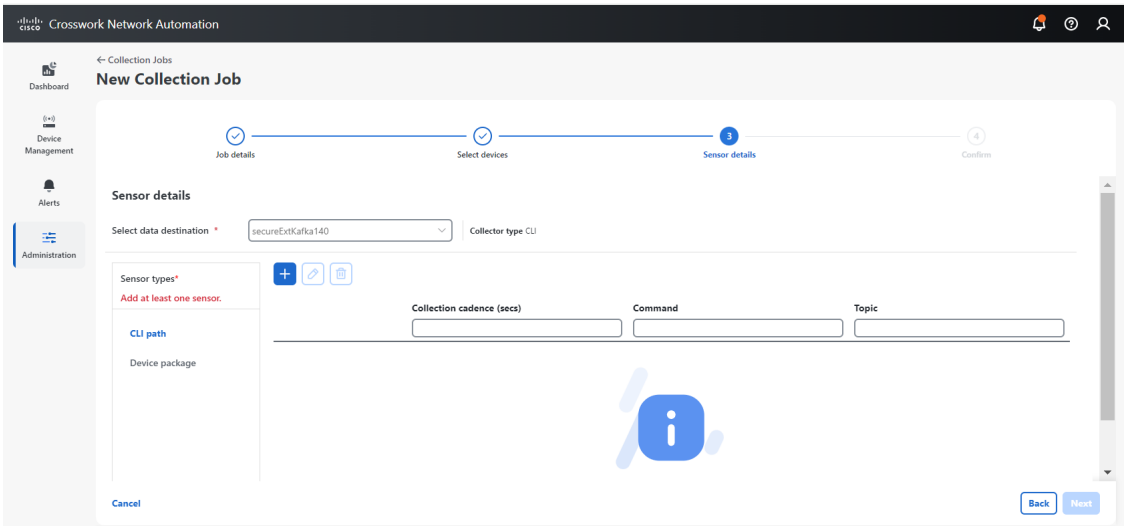


Figure 36: Add CLI path

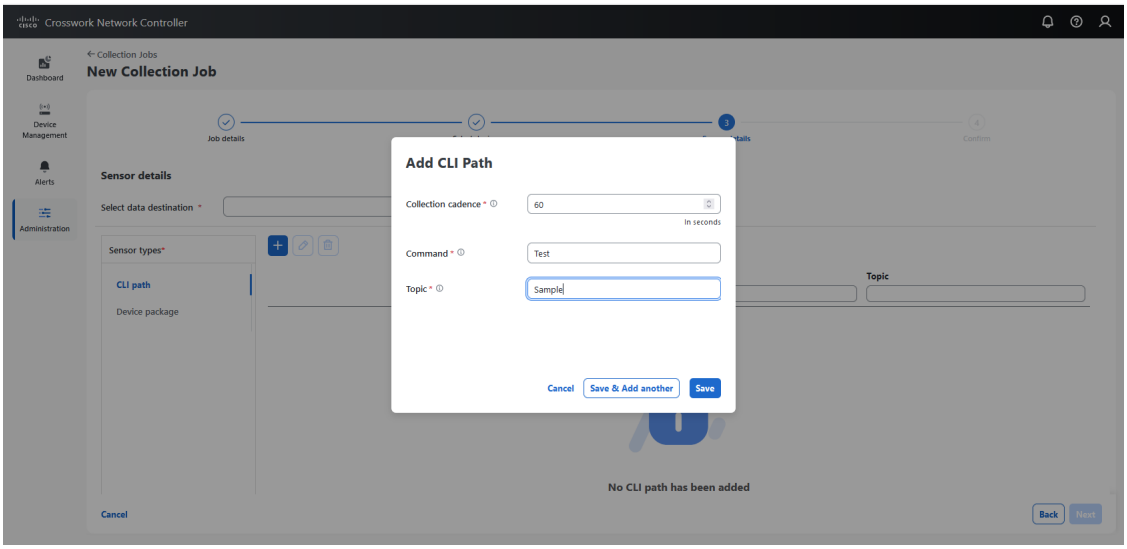


Figure 37: Add device package sensor

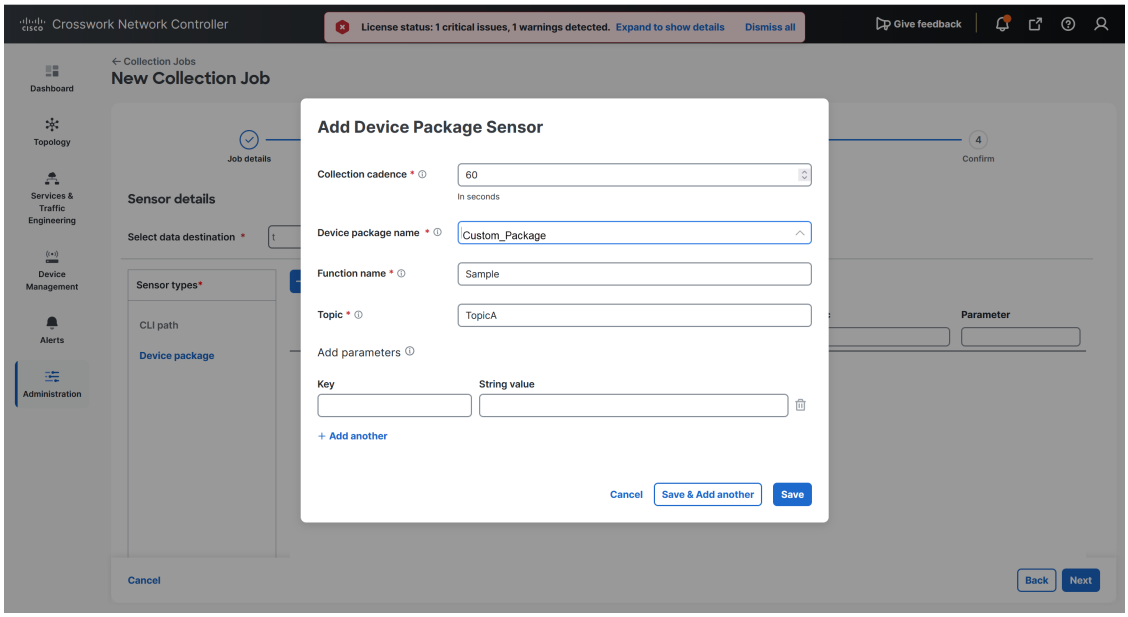


Figure 38: Sensor details for SNMP path

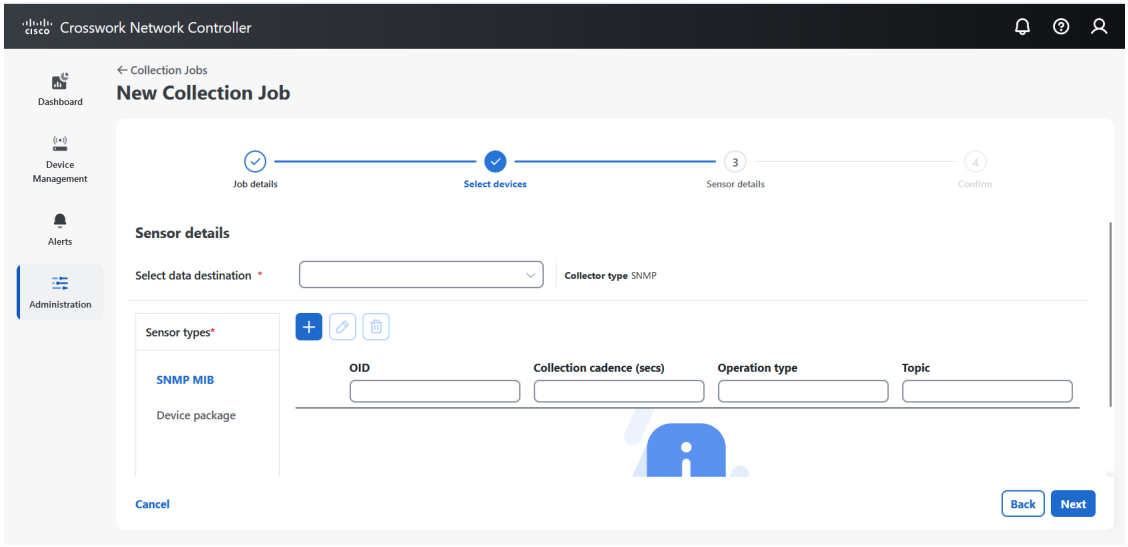
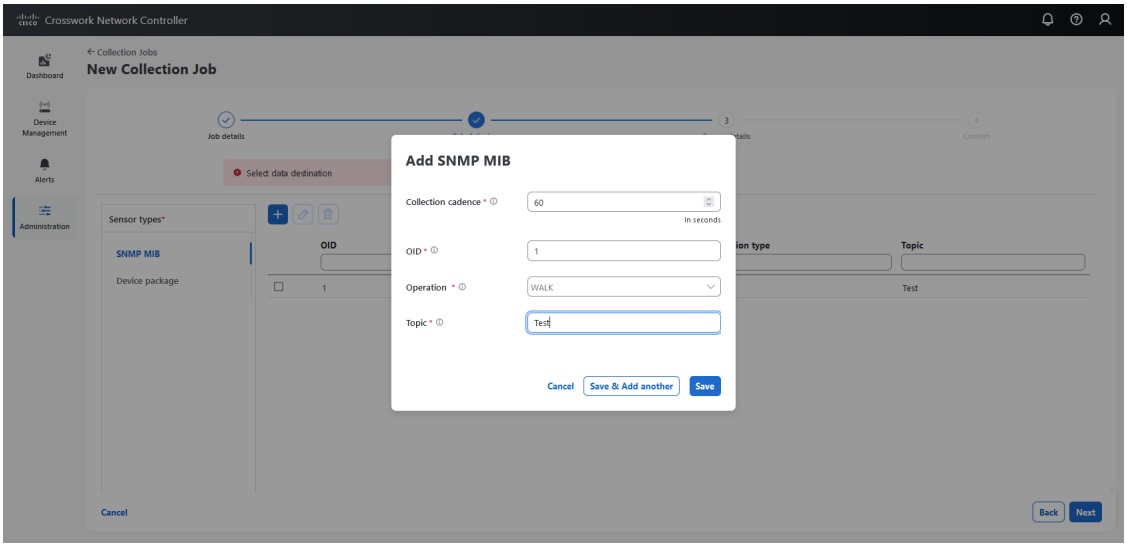


Figure 39: Add SNMP MIB



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 14: 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 105.

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

Table 15: 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 16: 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 111 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 129.

Supported trap types

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

Table 17: 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 18: 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 111.

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 133.
- Sample syslog collection payload, on page 136.
- 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 142.
- Secure syslog improves message integrity and confidentiality by using encrypted communication channels such as TLS. See Configure secure syslog on device, on page 137.

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.

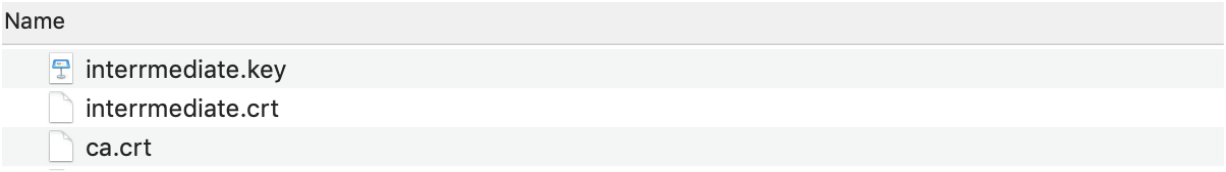
a. Access the Cisco Crosswork UI.

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.



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 19: 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 147.

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 148.

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 152.

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 154.

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

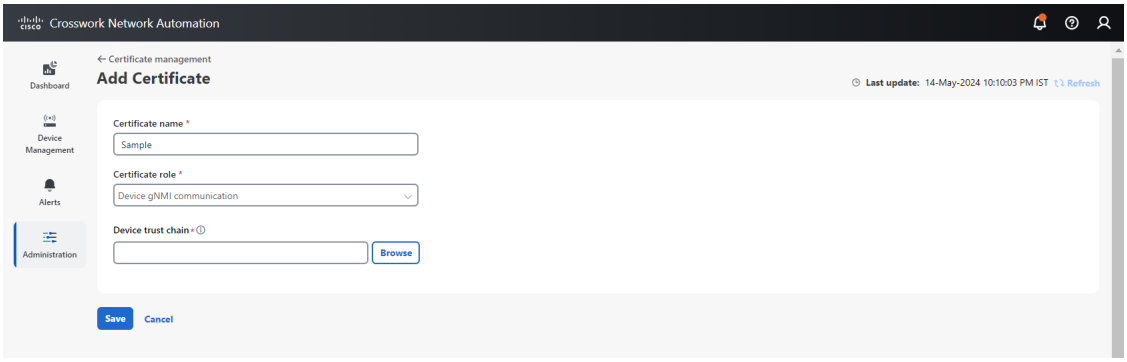
Step 1 From the Cisco Crosswork UI, go to **Administration > Certificate Management**.

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 40: Add certificate

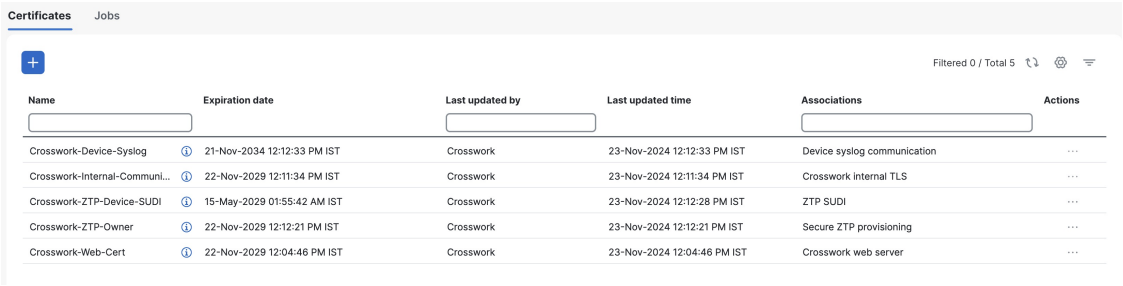


Note
If gNMI certificate is already configured and you wish to onboard a device with a different trust chain, update the existing .pem file to include details of the new CA. Select the existing gNMI certificate from the list, click the edit icon and upload the new .pem file.

Step 4 Click **Save**.

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

Figure 41: Certificates management



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 20: 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.

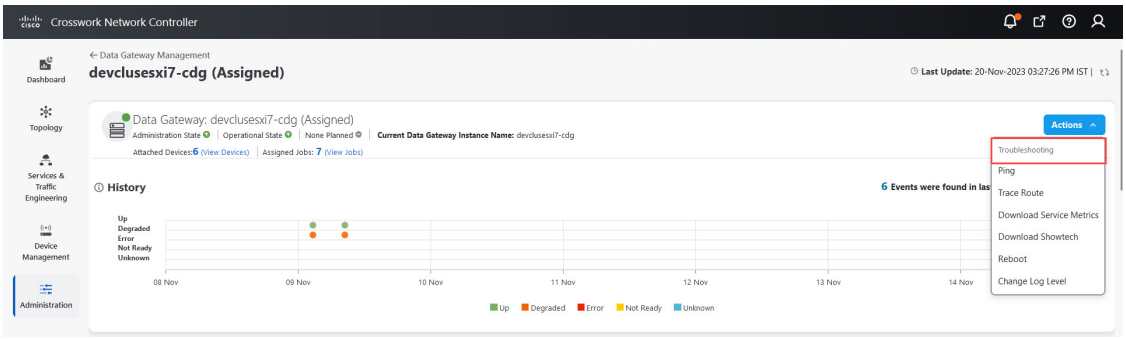
Use this section to access topics related to troubleshooting options and common issues in Crosswork Data Gateway.

- 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 155.
- 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 160.

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 42: Troubleshooting actions



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

- Check Data Gateway connectivity, on page 155
- Download service metrics, on page 85
- Download the showtech logs, on page 157
- Reboot Data Gateway VM, on page 86
- Change the log level of components , on page 159

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.

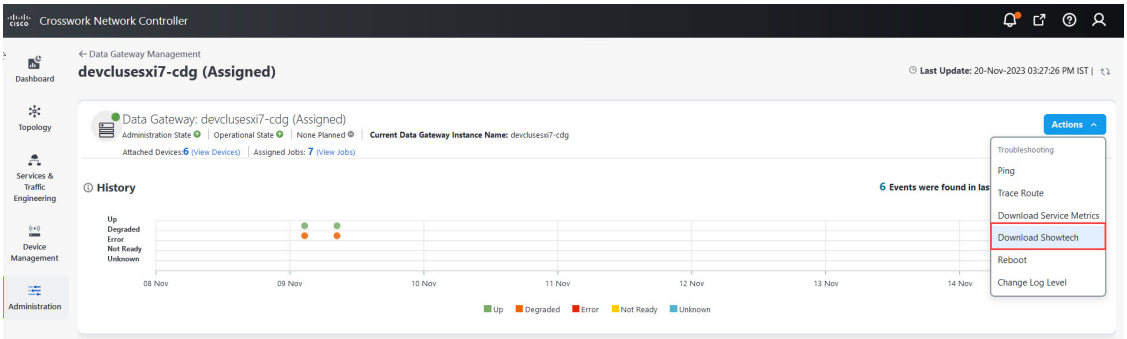
Procedure

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 43: Download showtech



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.

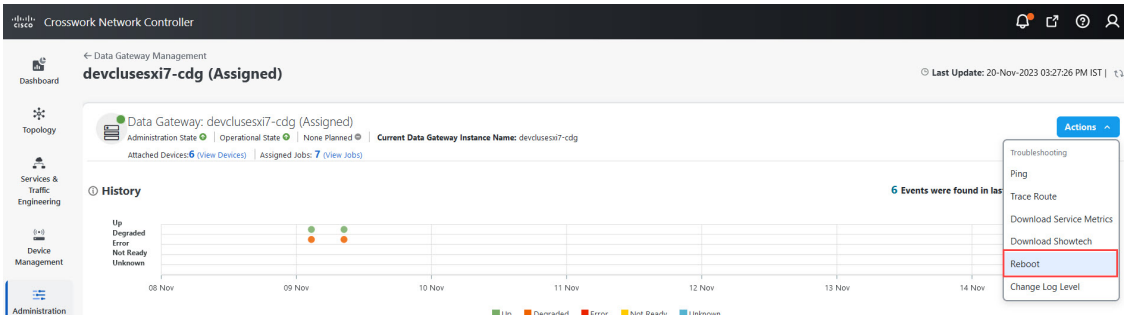
Procedure

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

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

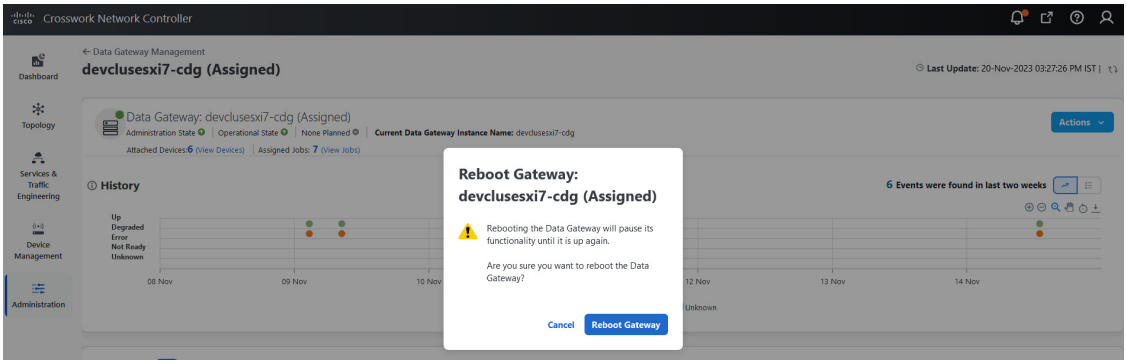
Step 3 On the **Crosswork Data Gateway details** page, at the top-right, click **Actions**, then click **Reboot**.

Figure 44: Data Gateway reboot



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

Figure 45: Reboot Data Gateway pop-up



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

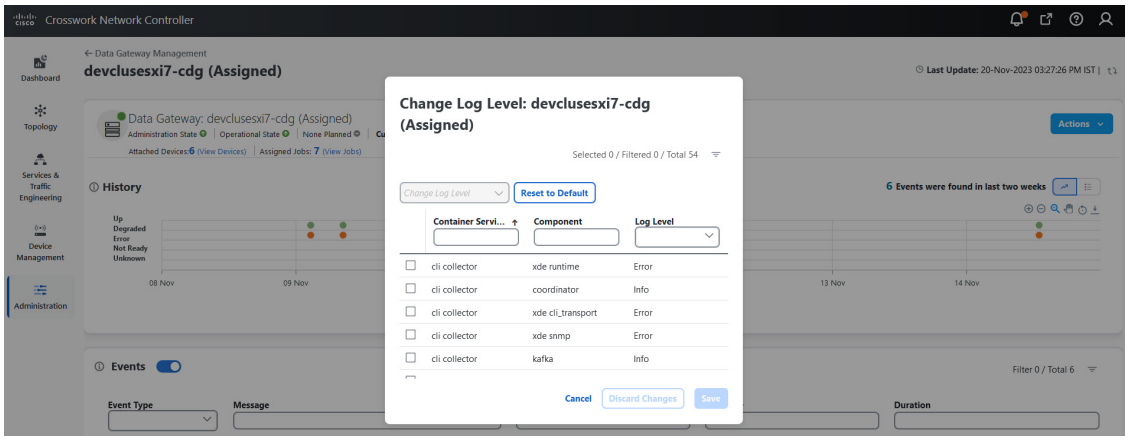
Step 1 Go to **Administration > Data Gateway Management > Data gateways**.

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 46: Change log level



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

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

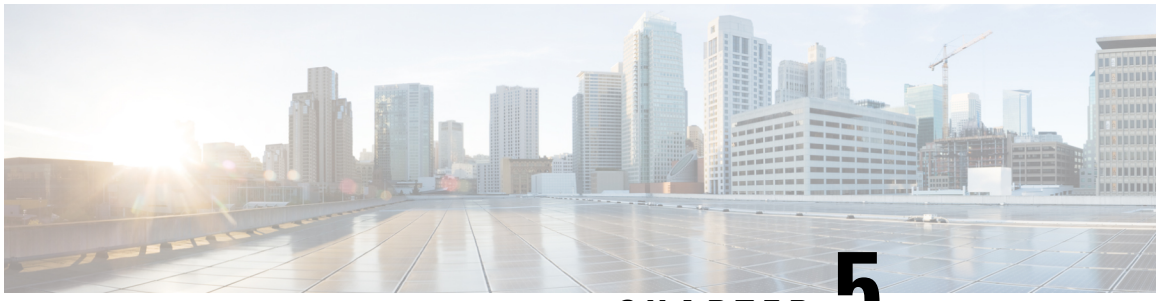
-

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.



CHAPTER 5

Embedded Collectors in single VM deployments

Embedded Collectors in Crosswork Network Controller

Embedded Collectors are included in the single VM deployment of Crosswork Network Controller. The solution collects network data via collector services and transfers it to Cisco Crosswork or external destinations using Kafka or gRPC. It is bundled with Cisco Crosswork Infrastructure and the Element Management Functions application as part of a unified package.

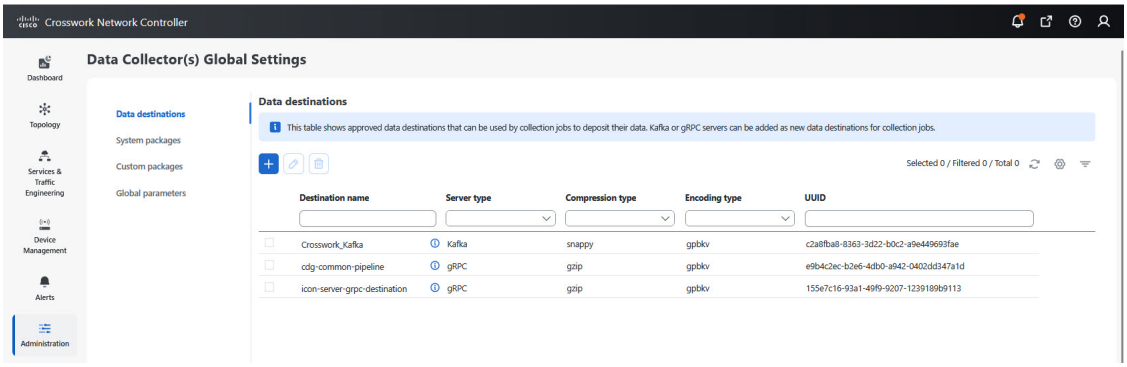
Key attributes:

- included with the bundled single VM deployment of Cisco Crosswork Network Controller
- collects network data from infrastructure devices using Embedded Collector services
- transfers data to Cisco Crosswork or external systems
- supports flexible data forwarding using Kafka or gRPC protocols, and
- enables streamlined integration with the overall Crosswork data and management ecosystem.

Access method for the Embedded Collector UI

You can access the Embedded Collectors through the management view from the **Data Collector(s) Global Settings** page in the Crosswork Network Controller UI.

Figure 47: Data Collector(s) Global settings



The Data Collector(s) Global Settings page allows you to perform the following administrative operations:

- **Data destinations**: After collecting the telemetry data, the collectors deposit it to an internal or external data destination. By default, `Crosswork_Kafka` is an internal data destination. You can define the external destinations using the Cisco Crosswork UI or APIs.

  To send data to external destinations using collection jobs, you must have an additional license. Make sure that the appropriate license is activated before configuring collection jobs. For the licensing details, see Licensing requirements for external collection jobs, on page 168.

- **Device packages**: By using device packages, the collectors can extend the data collection capabilities for both Cisco applications and third-party devices. The collectors support system and custom packages.
  - **System packages**: The system device package includes several installation files that are delivered via an application-specific manifest file. Usually, the manifest file is in JSON format.
  - **Custom packages**: The collectors user interface enables you to configure the port numbers of the collector pods. These port numbers affect the data collection services.
  - **Global parameters**: The collectors user interface allows enables you to configure the port numbers of the collector pods, which affect the data collection services. From this window, you can also enable the resync operation that automatically syncs the USM details whenever change occurs.

Configuring data collections in Embedded Collectors

Before setting up the Embedded Collectors, you must understand how Crosswork is set up. For more information, see *Tasks to complete for initial setup* section in the *Set Up Crosswork Network Controller* chapter.

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

Summary

This process explains how to configure Embedded Collectors 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.

Workflow

The data collection process involves these stages:

1. Complete the Single VM deployment: This package bundles Cisco Crosswork Infrastructure, Embedded Collectors, and Element Management Functions. This integration eliminates the need for separate installation. For more information, see the *Install Cisco Crosswork Network Controller on a Single VM* chapter in the *Cisco Crosswork Network Controller 7.2 Installation Guide*.
2. (Optional) Extend Embedded Collectors capabilities:

   This stage describes optional configurations that extend the Embedded Collector capabilities.

Table 21: Setting up data collection in Embedded Collectors

When the user wants to....	Then refer to the steps in...
1. Verify that default collection jobs are running.	Check the health status of Embedded Collectors , on page 233
2. (Optional) Add device packages to support additional or third-party devices	Device packages, on page 179
3. (Optional) Configure external data destinations	Data destinations in Embedded Collectors, on page 167
4. (Optional) Create custom collection jobs as needed	Collection jobs and supported protocols , on page 188

Result

When the process is complete, Embedded Collectors transmit collected data to the Crosswork Network Controller and other configured applications. You can enable advanced features to extend data collection capability.

Data destinations in Embedded Collectors

A data destination in the context of Embedded Collectors is a component in the Crosswork infrastructure that

- serves as the endpoint where collected network telemetry and performance data from Embedded Collectors is sent for processing, storage, and analysis,
- in a single VM deployment, is typically the local Crosswork data processing engine co-located within the same VM along with Embedded Collectors, forwarding data through internal buses or message brokers to processing services, databases, and analytics engines, and
- equires configuration with accurate IP addresses/hostnames, port numbers, authentication credentials, and protocol specifications (such as gRPC, TCP, UDP), while respecting system resource constraints and network connectivity rules to ensure optimized performance and reliable data flow.

Licensing requirements for external collection jobs

To set up collection jobs that send data to the external destinations, you need extra license. We recommend installing the license before configuring Crosswork to use an external destination. If you don't install the license first, you can still use the feature for 90 days under the trial license before it gets disabled.

When the License Authorization Status is "Out of Compliance", Crosswork Network Controller continues to allow users to create new external collection jobs and to view or delete existing jobs. This state occurs if registration with Cisco Smart Software Manager is not completed after the evaluation period or if the device limit for external collection jobs is exceeded.

View the license status

Check whether your system is properly registered and authorized to use licensed features.

Use this task when you need to confirm that your system has an active license, is in compliance, and is enabled for reserved features. This ensures ongoing access and compliance with Cisco Smart Software Manager requirements.

Procedure

Step 1 Go to **Administration > Smart Licenses**.

The **Smart licenses** tab under the **Application management** page is displayed.

Step 2 Ensure that the status is as:

- Registration Status: Registered. Indicates you have registered with Cisco Smart Software Manager (CSSM) and are authorized to use the reserved licensed features.
- License Authorization Status: Authorized (In Compliance). Indicates you have not exceeded the device count in the external collection jobs.
- Under Smart Licensing Usage, the entry "CNC Collection RTM - External Application End-Point" should show a status of In Compliance.

Managing data destinations

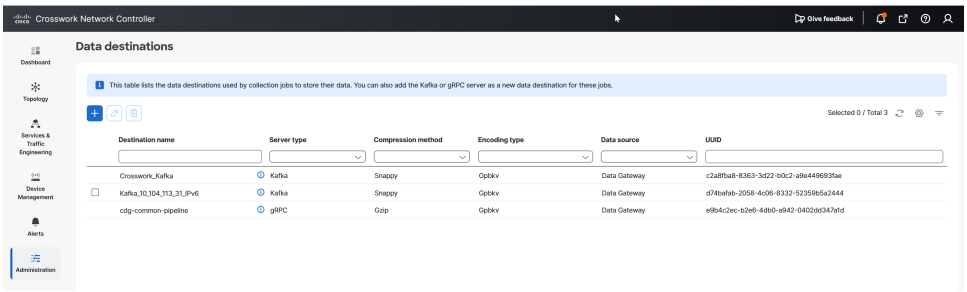
Explain how to manage external data destinations in Cisco Crosswork, including creating, modifying, and selecting data destinations for telemetry collection jobs.

Cisco Crosswork enables the creation of external data destinations, such as Kafka or external gRPC, which are utilized by the collection jobs to deposit the telemetry data.

To manage the data destinations, you can navigate to **Administration > Data Destinations**. From there, you have the options to

- add or modify a data destination
- delete any unused destinations, and
- view all the configured destinations.

Figure 48: Data destination



UUIDs for data destinations

The UUID is the unique identifier for the data destination. Cisco Crosswork automatically generates this ID when you create an external data destination.

When you create collection jobs using the Cisco Crosswork UI, you select the data destination from a drop-down list of configured destinations. When using the API, you need to know the UUID of the destination where the collector sends its data.

Add or edit a data destination

Add a new data destination or modify an existing one, enabling Embedded Collectors to send collected data to the desired destination.

Use this procedure to direct collected data to a new location or to update the parameters for an existing data destination, such as Kafka or gRPC endpoints.

Before you begin

Review the prerequisites and ensure you have all required information, such as destination details and authentication requirements.

Procedure

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

Step 2 On the **Data destinations** page:

a) To add a new destination, click **+ Add another**. Repeat this step for each additional collector. The **Data destinations** page opens.

b) To edit an existing destination, select it and click . The **Edit destination** page opens showing the current parameters. Update them as needed.

Note
When you update a data destination, the collector using it establishes a new session with that destination. Data collection pauses and resumes once the session is restored.

Step 3 Enter or update the required values for your external destination. If you are unsure about a value, use the default settings. For parameter information, see Parameters for adding and editing data destinations, on page 173.

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 **Collector**.

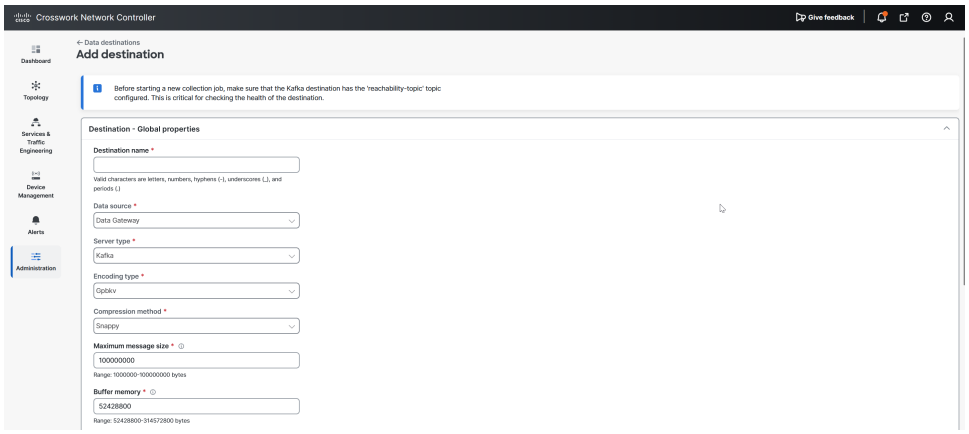
b) Enter values for all required fields.

- **Custom buffer memory**
- **Custom batch size**

  Note
  The **Custom batch size** cannot exceed the value of the **Custom buffer memory** at run time. If you do not enter a value for **Custom buffer memory**, validation occurs against the global Buffer Memory value.

- **Custom linger time**
- **Custom request timeout**

Figure 49: Add destination



c) Click **+ Add Another** to repeat for additional collectors.

Note
Properties set here override the global settings for the selected collectors. If you leave a field blank, the global properties are used.

Step 5 Select the protocol and host details in the **Connection details** sections. The supported protocols are IPv4, IPv6, and FQDN. For connection parameters, see Parameters for adding and editing data destinations, on page 173.

Note
FQDN is supported only for Kafka destinations.

Step 6 Complete the fields in Connection Details according to your connectivity type. Ensure the values match those configured on the external Kafka or gRPC server.

Note
You can change port numbers only for user-defined destinations. The ports of system-created destinations cannot be modified.

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.
- **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 For Kafka or gRPC-based destinations, select an authentication option:

- **Mutual-authentication**: Authenticates both server and Embedded Collectors after uploading CA certificate and Intermediate certificate or Key. (Default)
- **Server-authentication**: Authenticates both external server and Embedded Collectors using the CA certificate only.

Note
Authentication options are available only when **Enable secure communication** is enabled.

Step 9 Click **Save**.

The new or updated data destination is saved. The Embedded Collectors send data using the new configuration.

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 enabled secure communication, go to the **Certificate Management** page of your Crosswork UI and add the relevant certificate for the data destination. This step is required to establish secure communication.

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.

Requirements to add data destination

To use an external Kafka server as a data destination in Embedded Collectors, 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 Kafka server properties: Set these properties on your external Kafka server:
  - `num.io.threads = 8`
  - `num.network.threads = 3`
  - `message.max.bytes= 30000000`

  Refer to Kafka documentation for detailed descriptions and usage of these properties.
- Configure data destinations
  - You can configure multiple data destinations as needed.
  - If you reinstall an existing external Kafka destination using the same IP address, restart the collectors for changes to take effect.
- Validate connectivity and custom properties
  - Verify port connectivity for each data destination. If the port is unreachable, the collection will fail.
  - Embedded Collectors support custom values in Kafka destination properties. This customization feature is not supported for gRPC destinations.
  - Global properties entered in the Destination Details pane are mandatory and applied to all Kafka destinations by default unless overridden at the individual collector level.
- Secure communication (Optional)

  You can secure communication between Crosswork and the Kafka data destination (either Crosswork Kafka or external Kafka). Note that encryption can impact performance.

  If TLS is required:
  - Keep the public certificate ready for TLS verification.
  - For client authentication, keep the client certificate and key files available.
  - If the key file is password-protected, configure the password as part of destination provisioning.
  - Embedded Collectors currently support IP-based certificates only.

    Ensure that:
    - Certificates are PEM-encoded.
    - Key files are in PKCS#8 format when generated using a Certificate Authority.

Parameters for adding and editing data destinations

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

These parameters are grouped in two categories:

- General configuration parameters: Core options that affect the identity and encoding of the data destination.
- Connection configurations: Addressing and connectivity options, such as IP addresses or hostnames and ports.

Table 22: General configuration parameters for data destinations

Field	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.	Yes	Yes
Server type	Select the gRPC or Kafka for your data destination from the drop-down.	Yes	Yes

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

Field	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 the data source as • **Data Gateway**: destination exclusively used by Crosswork Data Gateway for telemetry and network data collection. • **Application**: destination exclusively used by Crosswork applications such as application events, alerts, and notifications. • **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. • Embedded collectors does not monitor the availability of Kafka destinations configured with the dispatch source as **Applications** (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 Gateway**. • Destinations that have **Application** as		

Field	Description	Available in gRPC	Available in Kafka
	the data source are removed after the upgrade.		
Encoding type **Note** This field appears only when the data source is set to Data Gateway or Any.	Choose encoding as Json or Gpbkv.	Yes	Yes
Compression method	Choose the compression method. Default is `snappy`. • Kafka supports `snappy`, `gzip`, `zstd`, `none` (zstd: Kafka ≥2.0). • gRPC supports `snappy`, `gzip`, `deflate`.	Yes	Yes
Maximum message size	Enter the max message size in bytes. • Default Value: 100,000,000 (100 MB). • Min: 1,000,000 (1 MB) • Max: 100,000,000 (100 MB).	No	Yes
Buffer memory	Enter required buffer memory in bytes. • Default Value: 52428800 bytes/52.4288 MB • Min: 52428800 bytes/52.4288 MB • Max: 314572800 bytes/314.5728 MB	No	Yes
Batch size	Enter required batch size in bytes. • Default Value: 1048576 bytes/1.048576 MB • Min: 16384 bytes/16.38 KB • Max: 314572800 bytes/314572.8 KB	No	Yes

Field	Description	Available in gRPC	Available in Kafka
Linger time	Enter linger time in ms. • Default Value: 2000 ms • Min: 0 ms • Max: 5000 ms	No	Yes
Request timeout	Enter request timeout duration in seconds. • Default Value: 30 seconds • Min: 30 seconds • Max: 60 seconds	No	Yes

Note

- For fields with limits, abide by min/max/default values to prevent configuration errors.
- Some parameters are only available for Kafka destinations, not for gRPC (e.g., buffer memory, batch size).
- Use informative names for easier management if you have many data destinations.

Table 23: Connection configuration parameters for data destinations

Field	Description	Available in gRPC	Available in Kafka
IPv4	Enter IPv4 Address/Subnet Mask and Port. Add multiple IPv4 addresses via **+ Add another** • Subnet mask: 1–32 • Port: 1024–65535	Yes	Yes
IPv6	Enter IPv6 Address/Subnet Mask and Port. Add multiple IPv6 addresses via **+ Add another**. • Subnet mask: 1–128 • Port: 1024–65535 IPv6 subnet mask ranges from 1 to 128 and ports range from 1024 to 65535.	Yes	Yes
FQDN	Enter Host Name, Domain Name, and Port (1024–65535). Add multiple via **+ Add another**.	Yes	Yes

Note Additional details:

- For all connection fields, you can add multiple entries using the **+ Add another** option.
- Always verify firewall settings to allow configured ports.
- Supported port ranges apply consistently across IPv4, IPv6, and FQDN settings.

View the data destination details

Review the configuration and attributes of a selected data destination within the Data Gateway.

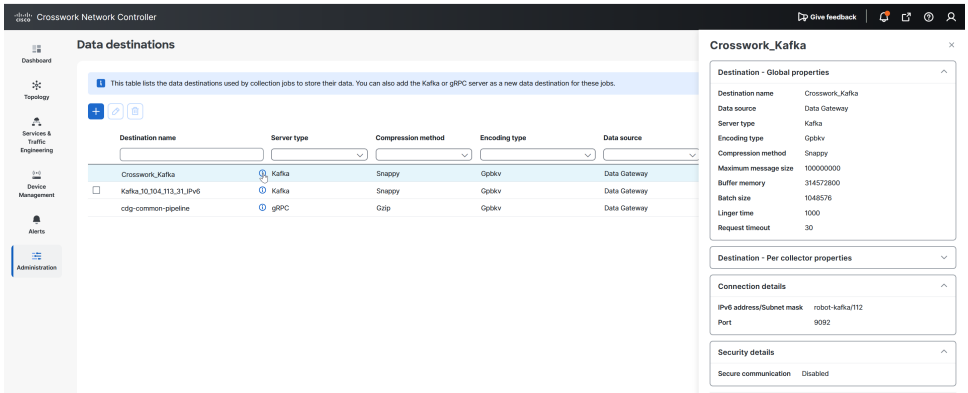
Use this task when you need to audit, verify, or analyze the data destination endpoints configured for your organization. Accurate review ensures that data flows to intended endpoints and assists in diagnosing configuration or routing issues.

Procedure

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

Step 2 Click the icon next to the data destination whose details you want to review.
Destination details appear with associated configuration information.

Figure 50: View destination details



The details for the selected data destination are displayed, allowing you to verify attributes and configuration.

What to do next

After viewing, confirm that the data destination matches the desired configuration. If you find any discrepancies, adjust the settings. If there are no discrepancies, continue regular monitoring.

Delete a data destination

Delete one or more data destinations from the system.

Data destinations store information collected by the data collector. You may need to delete a destination if it is no longer needed or to maintain system hygiene.

Before you begin

- A data destination can only be deleted if it is not associated with any collection job. Deleting a destination also removes all associated data subscriptions.
- Default destinations, such as `Crosswork_Kafka`, cannot be deleted.
- Check the **Collection Jobs** view to determine if any collection jobs are using the data destination.

Procedure

Step 1 Got to **Administration** > **Data Destinations**.

Step 2 Select one or more data destinations to delete from the displayed list.

Step 3 Click  .

Step 4 In the **Delete Data Destination(s)** pop-up, click **Delete** to confirm.

The selected data destinations are deleted from the system.

What to do next

Verify the destination has been removed.

Device packages

A device package is a data collection framework that

- defines communication protocols including commands, telemetry models, and SNMP objects required to retrieve device data from network devices
- translates device data into a standardized format for downstream processing within Embedded Collectors, and
- enables multi-vendor support allowing Embedded Collectors to communicate with multiple device types and vendors without requiring additional code changes.

Types of device packages

Embedded Collectors use device packages to define communication and data collection from network devices. These are categorized as system packages and custom device packages.

- System packages are preinstalled packages that ship with Crosswork. They include built-in definitions for Cisco and commonly supported third-party devices. These packages contain the standard CLI, SNMP, and telemetry collection models required for those devices.

  System device packages have these characteristics.

  - Installed automatically with Embedded Collectors.
  - Maintained and updated by Cisco.
  - 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.
  - Updated as part of Embedded Collectors or device package version upgrades.

  System packages ensure that Embedded Collectors can immediately begin collecting data from supported devices without requiring manual configuration.

- Custom device packages are provided by administrators. They extend the data collection capabilities of Embedded Collectors beyond the coverage of system packages. Typically, administrators use these to onboard unsupported devices, add vendor-specific MIBs, or introduce additional metrics.

  Custom device packages have these characteristics.

  - Created, imported, or obtained separately (for example, from Cisco or third-party vendors).
  - Uploaded manually through **Administration > Data Gateway > Device Packages**.
  - Can be edited, replaced, or deleted by administrators as needed.
  - Useful for integrating proprietary, non-Cisco, or newer device types.

Note Custom packages co-exist with system packages and take precedence when both define the same device type or data model.

Download system packages

Download system packages that are relevant for an application using the system's administration interface.

System packages are provided through an application-specific manifest in JSON format. They are centrally managed and updated whenever applications are installed or upgraded.

Before you begin

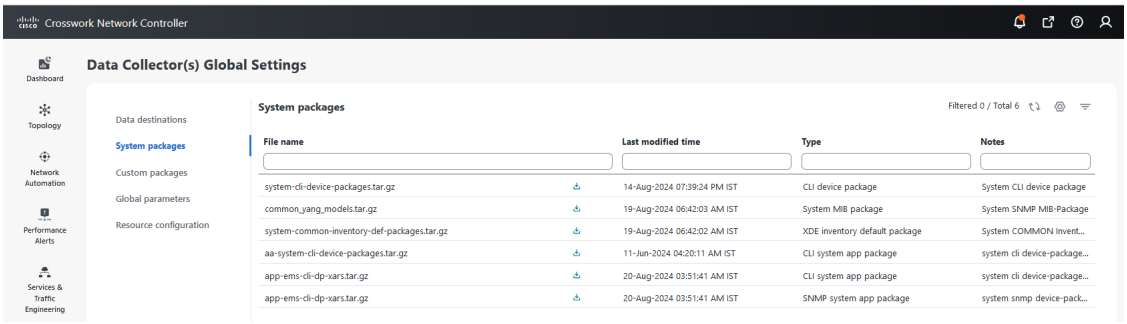
Identify the system package you need to download.

Procedure

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

You will see the System Packages window.

Figure 51: System Packages Window



Step 2 Click the ⬇ button located next to the package name in the **File Name** column.

The selected system package is downloaded and available for use.

What to do next

Confirm the file has downloaded successfully.

Custom packages

A custom package is a bundle that

- enables user-supplied extensions for device communication and data collection
- allows integration of third-party device models and data formats, and
- supports enhanced monitoring and management within Crosswork Network Controller.

Types of custom packages

You can upload these types of custom packages to Crosswork Network Controller:

- CLI Device Package: Monitors device health for third-party devices using KPIs based on the CLI. All packages and their corresponding YANG models must be included in the `custom-cli-device-packages.tar.xz` file.
- Custom MIB Packages: Contains custom MIBs and device packages designed for third-party devices, and filter or format collected data for Cisco devices. You can edit these packages, which must be included in the `custom-mib-packages.tar.xz` file. The system supports only one custom MIB package.
- SNMP Device Package: Extends SNMP coverage via custom SNMP device packages in `.xar` format, using Embedded Collectors.
- Aggregate Package: Enables you to include multiple supported file extensions in one package. You can upload and download aggregate packages using the Crosswork UI.

Supported file extensions for aggregate packages

Aggregate packages may contain these file types:

- Collector file
  - YANG (.yang)
  - MIB (.mib, .my)
  - Definition (.def)
  - Device packages (.xar)
- Application files
  - Device-metadata (.yaml, .yml)
  - Zips (.zip)
  - SDU bundle (.sdu)

Requirements for proprietary MIBs

Proprietary MIBs are only needed when collection requests reference MIB TABLE names or SCALAR names from a proprietary MIB. If requests use OIDs, proprietary MIBs are not required. Standard MIBs are already included in the system for SNMP polling on third-party devices.

Upload the custom package

Add a new custom package to the system by uploading a prepared tar.gz bundle.

Custom packages allow administrators to introduce new capabilities or configurations by uploading bundled resources in a standard archive format. Supported package types include those for SNMP and CLI collectors.

Before you begin

Review the requirements and ensure that you meet the requirements.

Procedure

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

Step 2 On the **Custom packages** page, click  .

Step 3 In the **Add custom packages** window, select the appropriate package type from the **Type** dropdown.

Step 4 In the **File name** field, click to open the file browser, select your tar.gz custom package, and click **Open**.

Step 5 Add a description of the package in the **Notes** field. We recommend including a unique description for each package to easily distinguish between them.

Step 6 Click **Upload**.

The system processes your upload and adds the custom package to the selected collector or gateway. Confirmation is shown upon completion.

Requirements to upload custom packages

Ensure that all prerequisites are met and review the applicable upload restrictions before uploading custom packages. Observe these requirements:.

- MIB package dependencies: Ensure that the new MIBs include all necessary dependencies in the bundle to prevent import errors.
- Supported file extensions: The package must include only supported file types. For the complete list of supported extensions, see the referenced documentation.

  Supported file extensions: The package must include only supported file types. For the full list of supported extensions, refer to the relevant documentation. For a full list of supported extensions, see Custom packages, on page 181.
- Package format: Bundle all the package contents into a `.tar.gz` archive before uploading.
- Collector types: The archive must include at least one of the top-level directories:
  - `cli/`
  - `snmp/`
  - `common/`

  See Sample package directory structure, on page 184 for the recommended directory structure.
- To update a CLI package, click the Upload icon next to the filename on the Custom Packages page. This action replaces the existing file.
- When uploading multiple files, combine multiple `.xar` files into a single `.tar.gz` archive before uploading.

Performance considerations for uploading custom packages

Before uploading custom MIBs and YANGs to the Crosswork Network Controller, ensure that your packages are thoroughly performance-tested and optimized for your deployment scale.

- Optimize custom package efficiency to improve collection job performance.
- Test package performance prior to uploading to ensure compatibility and scalability for your environment.

For detailed validation instructions on custom MIBs and YANGs, refer to Cisco DevNet documentation.

Restrictions and validations for custom package uploads

Observe these restrictions and validations when uploading custom packages:

- Do not attempt to overwrite system MIBs with custom MIBs; this action is not supported and will result in a failed upload.
- Package archive requirements:
  - Include only the directories `cli/`, `snmp/`, and `common/` at the root level of the `.tar.gz` archive.
  - Avoid including parent folders or extra hierarchy levels to prevent exceptions during job execution.
- Crosswork validates only file extensions at upload time; file contents are not validated.

Sample package directory structure

This example shows a 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
```

Delete the custom package

Remove a custom package from Cisco Crosswork and delete associated files.

Deleting a custom package automatically removes all YANG and XAR files associated with it and affects any collection tasks that rely on it.

Procedure

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

Step 2 In the **Custom Packages** pane, select the package you want to delete.

Step 3 Click  .

Step 4 In the **Delete Custom Package** window that appears, click **Delete** to confirm.

Global collector parameters

Global settings define how the collectors operates and integrates with other network components such as devices, data destination. These configurations offer a centralized way to manage key operational parameters consistently across the Embedded Collectors.

The primary functions of global configuration options include:

- Controlling how Embedded Collectors connect to external systems. See Data destinations in Embedded Collectors, on page 167.
- Extending data collection capabilities to Cisco applications and third-party devices using device packages. See Device packages, on page 179.
- Setting default thresholds, ports, timeouts, and retry limits. See Configure the global parameters, on page 185.

Configure the global parameters

Guide users to configure global parameters for collectors in the network management system.

The Global Parameters window enables configuration of foundational operational settings for collectors, such as specifying data collection ports. Update these settings if your network uses non-standard ports to maintain proper collector integration and operation.

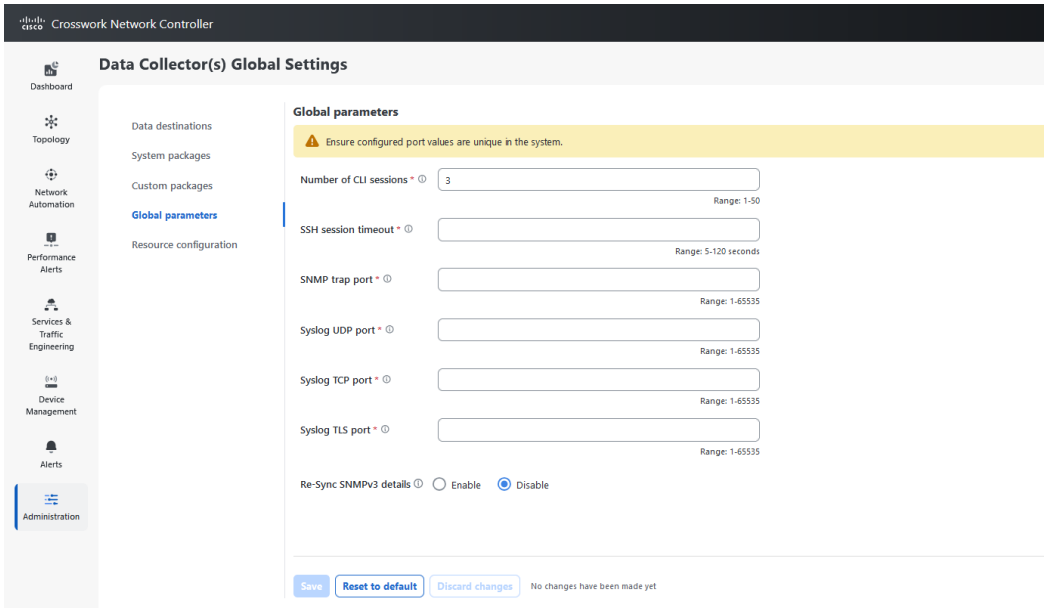
Before you begin

- Ensure port values you intend to update are valid and do not conflict with existing assignments.
- Confirm port numbers match those configured on your devices
- Ensure port values do not conflict with those on Embedded Collectors.
- Changes to Syslog and SNMP ports will apply to Embedded Collector instances running on Amazon EKS.

Procedure

Step 1 Navigate to **Administration > Data Collector(s) Global Settings > Global Parameters**.

Figure 52: Global parameters



Step 2 Update the parameter values as per your network requirement.

Step 3 If you are updating ports, select **Yes** in the **Global Parameters** window that appears to confirm that collectors can be restarted.

Note
Updating ports causes the collectors to restart and pause any collection jobs that are running.

Step 4 Click **Save**.

A confirmation message indicates whether the update succeeded or failed for Embedded Collectors.

What to do next

If any Embedded Collectors cannot be updated, an error window appears. During recovery, these collectors will automatically retry parameter updates; some may restart as part of this recovery process.

Note One reason global parameters might fail to update on an Embedded Collector is that the OAM channel is down. After the OAM channel is reestablished, Embedded Collectors attempt to send the parameters to the unsynchronized collectors, updating the values after comparing them with the existing ones.

Global parameters and descriptions

This section lists the global parameters and descriptions.

Note The port number you modify must match the numbers configured on your devices.

Table 24: Global parameters and descriptions

Parameter Name	Description	Default value for single VM deployment
Number of CLI sessions	Maximum number of CLI sessions that can be set up between an embedded data collector and devices. Change this value to increase or decrease the number of concurrent sessions allowed on the device, depending on requirements.	3 Accepted range is 1-50
SSH Session Timeout	The session timeout (in seconds) is the duration for which a CLI connection can remain idle in the CLI and SNMP collectors.	120 Accepted range is 5-900 seconds
SNMP Trap Port	Modify this value according to the deployment environment and configuration requirements.	31062 Accepted range is 30160–31560
Syslog UDP Port	Modify this value according to the deployment environment and configuration requirements.	30514 Accepted range is 30160–31560
Syslog TCP Port	-	30898 Accepted range is 30160–31560
Syslog TLS Port	-	30614 Accepted range of ports is 30160–31560

Parameter Name	Description	Default value for single VM deployment
Re-Sync SNMPv3 Details	USM details change whenever a device is rebooted or re-imaged. 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 USM (User Session Manager) information is not permitted to prevent unintended data collection with 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, manual intervention is required to re-establish USM communication. This process can be performed by detaching and reattaching the device to the embedded collectors or toggling the device's admin state (Down then Up).

Collection jobs and supported protocols

A data collection process is a mechanism that

- enables applications to request network data through collection jobs
- allows the Crosswork Network Controller to assign these jobs to an appropriate collector, and
- ensures that the collector initiates and performs data collection based on the type of data requested.

The Embedded Collector collects data using supported protocols such as CLI, SNMP, gNMI (dial-in), and syslog. It can collect any type of data if it is able to forward it through one of these supported protocols. Embedded Collectors offer flexibility in data collection by supporting multiple protocols. This capability ensures compatibility with diverse data types and network devices.

Types of collection jobs

There are two types of data collection requests in Crosswork Network Controller:

1. A data collection request forwards data for internal processes within Cisco Crosswork. Cisco Crosswork creates system jobs for this purpose. If you want the Embedded Collectors to collect specific information from non-Cisco devices, you must use custom device packages. For more information about custom device packages, see Custom packages, on page 181.

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

2. Data collection request to forward data to an external data destination. For more information about configuring the external data destinations (Kafka or gRPC), see Data destinations in Embedded Collectors, on page 167.

Supported types of collection jobs

- CLI-based collection
- SNMP-based collection
- Syslog-based collection
- gNMI-based collection

For each collection job you create, Embedded Collectors execute the collection request and forward the data to both internal and external destinations. A single collection request allows you to send the collected data to the Crosswork Network Controller and to an external data destination.

You can create collection jobs from the Cisco Crosswork Network Controller UI. You can also use APIs to create jobs, see Cisco DevNet. For example, you may create an SNMP-based collection job to regularly retrieve interface statistics from a device and deliver data to both the controller and an external monitoring server.

How collection job state transitions work

Collection jobs progress through distinct status stages, beginning with creation and ending with execution in the Crosswork system.

Summary

Collection jobs transition through distinct status stages as they move from creation to execution within the Crosswork system.

The key components involved in the process are:

- Collection job: the request that is created to collect data.
- Embedded Collector: the collector that validates and executes jobs.
- Crosswork Network Controller UI: the management interface where users monitor job status.

Workflow

The process involves these stages:

1. Initially, every collection job appears in the UI with the status Unknown.
2. The Embedded Collector receives the collection job and performs basic validation checks.
3. If the job passes validation, its status changes to Successful.
4. If the job fails validation, its status changes to Failed.

Result

Users can track and manage the lifecycle of collection jobs. They can quickly see whether their jobs have succeeded, failed, or are waiting to be processed.

Status changes in event-based collection jobs

These scenarios illustrate how status changes appear in event-based collection jobs.

- When data collection is successful, the status of the collection job changes from Unknown to Success in the Collection Jobs pane.
- When a device is detached from Embedded Collectors, all corresponding collection jobs are deleted, and the job status is displayed as Success in the Collection Jobs pane. No devices or collection tasks are displayed in the Job Details pane.
- When a device is attached to an Embedded Collector, Crosswork receives a new collection job with the status set to Unknown, which changes to Success after events are received from the device.
- If the device configuration is updated incorrectly on an already attached device (and Embedded Collectors has received the job and events), there is no change in the status of the collection task in the Jobs Details pane.
- If device inventory is updated with an incorrect device IP, the collection task status in the Jobs Details pane remains Unknown.

CLI collection jobs

A CLI collection job in the Embedded Collectors is a data collection method that

- uses command-line interface (CLI) commands to retrieve operational or configuration data from network devices,
- enables collection of real-time information when devices do not support other protocols such as SNMP or gNMI, and
- supports troubleshooting and monitoring by ensuring critical data is available.

Best practice for devices with banner configurations

If a banner configuration is currently enabled on your device, refer to the device's official documentation for instructions on how to disable it.

How CLI jobs collect data

Summary

CLI collection jobs automate data collection from devices. They reference designated destinations and device identifiers using the CLI protocol.

Workflow

The key steps for configuring a CLI collection job are:

1. Configure a data destination: To create a custom CLI collection job, configure a data destination. Each destination receives a unique UUID, which is required as destination_id in API payloads. You can create a destination using **Data Collectors > Data Destinations**.
2. Identify the device. The device uses a UUID instead of an IP address for identification.
3. For jobs built using the UI, Crosswork Network Controller automatically retrieves required UUIDs. For custom jobs, retrieve UUIDs manually.

Result

Setting up a CLI collection job with correctly referenced destinations and devices enables streamlined and accurate CLI-based data collection in the network management system.

Cadence for data collection

Cadence is a configuration parameter that

- determines how frequently the Embedded Collectors collect data from each device
- accepts a range between 10 and 604,800,000 milliseconds, and
- allows the user to tailor the data collection rate to operational needs.

For example, a cadence value of 60,000 milliseconds (1 minute) means data will be retrieved every minute. The minimum recommended cadence is 60 milliseconds. Select an appropriate cadence to balance data granularity with system and network performance.

Best practice for setting data collection cadence

- Set a minimum cadence of 60 milliseconds for most data collection jobs.
- Use a higher cadence (slower rate) for collecting consistent data, such as memory consumption or CPU utilization.
- Use a shorter cadence (faster rate) to collect data points that are more dynamic and fast-changing.
- High-frequency collection can increase the load on both devices and the Crosswork Network Controller. Consider this impact when choosing a cadence.
- Experiment with different cadence values to find the optimal balance between actionable insight and system performance.

Considerations for skipped collection attempts

When a collection attempt is skipped because a previous execution is still in progress, Embedded Collectors issue a warning log. However, the system does not generate an alert for this scenario. This behavior prevents overlapping data collection processes and helps maintain operational efficiency.

Sample payload of CLI collection job

A sample payload is a structured example that demonstrates how device data can be sent to an external system using a defined schema. It clarifies the usage of system-assigned identifiers such as UUIDs and provides a template for integrating Crosswork jobs with external Kafka destinations.

The sample payload includes the structure and values used when Crosswork sends device data to an external Kafka destination. It uses the UUID assigned by the Device Lifecycle Manager..

For detailed information about the API payload fields and usage examples, see the API documentation on Cisco Devnet.

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "CLI_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "658adb03-cc61-448d-972f-4fcec32cbfe8"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "cli_sensor": {
            "command": "show platform"
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "sensor_output_configs": [
     {
        "sensor_data": {
          "cli_sensor": {
            "command": "show platform"
          }
        },
        "destination": {
          "destination_id": "1e71f2fb-ea65-4242-8efa-e33cec71b369",
          "context_id": "topic1"
        }
      }
    ]
  }
}
```

SNMP collection jobs

An SNMP-based data collection job is a process that collects device data using SNMP through Embedded Collectors configured via the UI or API. It retrieves data based on the device's Management Information Base (MIB) and associated Object Identifiers (OIDs). This collection can be configured in two ways:

- MIB-based polling, which gathers data according to the device's supported MIB and OID definitions, and

- Trap-based listening, which collects SNMP traps by configuring the collector to listen for incoming trap messages.

Standard MIBs included with Crosswork enable collection of common device attributes. Custom or vendor-specific MIB packages can be uploaded for specialized devices.

Supported SNMP versions for polling and traps include SNMP v2 and SNMP v3. These versions offer various authentication protocols (such as HMAC_MD5 and HMAC_SHA variants) and privacy protocols (such as AES, DES, 3-DES, and Cisco-specific AES). This approach enables a flexible and secure collection of network device data for monitoring and management.

Supported SNMP versions and operations

Supported SNMP versions for data polling and traps are

Polling data

- SNMP V2
- SNMP V3 (no auth nopriv, auth no priv, authpriv)
- Supported auth protocols: 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

- SNMP V2
- SNMP V3 (no auth nopriv, auth no priv, authpriv)

Sample SNMP device configuration commands

This table lists sample SNMP configuration commands for enabling polling and traps on V2 and V3 devices, including IP address, port notes, and authentication or naming requirements.

Table 25: Sample configuration to enable SNMP on device

Version	Command	Purpose
V2c	`snmp-server group <group_name> v2c` `snmp-server user <user_name> <group_name> v2c`	Defines the SNMP version, user or user group details.
	`snmp-server host <host_ip> traps SNMP version <community_string> udp-port 31062` `snmp-server host a.b.c.d traps version 2c v2test udp-port 31062`	Defines the destination to which trap data must be forwarded. **Note** The IP address must be the Data VIP address of the Embedded Collectors.
	`snmp-server traps snmp linkup` `snmp-server traps snmp linkdown`	Enables traps that notify about link status.

Version	Command	Purpose
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 31062`	Defines the destination to which trap data must be forwarded. **Note** The IP address must be the Data VIP address of the Embedded Collectors.
	`snmp-server user <user_name> <group_name> v3 auth md5 <password> priv aes 128 <password>`	Configures the SNMP server group and enables authentication for specified members in a named access list.
	`snmp-server view <user_name> < MIB > included`	Specifies the information that must be reported.
	`snmp-server group <group_name> v3 auth notify <user_name> read <user_name> write <user_name>`	Defines the SNMP version, user, or user group details.
	`snmp-server enable traps snmp [authentication ] [linkup ] [linkdown ] [warmstart ] [coldstart ]`	• When you use this command without any optional keywords, it enables authenticationFailure, linkUp, linkDown, warmStart, and coldStart traps. • When you include keywords with this command, it enables only the specified trap types. For instance, to enable only linkUp and linkDown SNMP traps for all interfaces, use the snmp-server enable traps snmp linkup linkdown command.

SNMP collector supported operations

- SCALAR
- TABLE
- WALK
- COLUMN

Notes for supported operations

- If a single collection requests for multiple scalar OIDs, you can pack multiple SNMP GET requests in a single `getbulkrequestquery` to the device.
- For TABLE operations, you can provide either a Table OID or a Column OID.
- There is an optional **deviceParams** attribute **snmpRequestTimeoutMillis** (not shown in the sample payloads) that should be used if the device response time is more than 1500 milliseconds.
  - Use **snmpRequestTimeoutMillis** unless you are certain that your device response time is high.
  - The value for **snmpRequestTimeoutMillis** should be specified in milliseconds:
  - The default and minimum value is 1500 milliseconds. There is no maximum value for this attribute.

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"
        }
      }
    ]
  }
}
```

SNMP traps collection job

SNMP trap collection jobs are created only through the API. Trap listeners monitor specific ports and dispatch data to recipients according to their topics of interest.

How SNMP trap collection jobs work

When the Embedded Collector receives an SNMP trap, it performs these actions:

1. Checks if any collection job is created for the device.
2. Checks the trap version and community string.

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

3. For SNMP v3, the system also validates the user authentication protocol, privacy protocol, and credentials.

Note SNMPv3 authentication and privacy traps depend on the engineId of the device or router to maintain the local USM user tables. If the engineId changes, trap collection is interrupted. To restore trap reception, detach the respective device and then reattach it.

Best practice for enabling SNMP traps

- Before starting the SNMP trap collection, install the Common EMS Services application and configure the host information for SNMP.
- Embedded Collectors listen on UDP port 31062 for traps.
- Before submitting SNMP trap collection jobs, ensure that SNMP traps are properly configured on the device and directed to the Data VIP address of the Embedded Collector.

Types of SNMP trap filters

Embedded Collectors filter traps using the trap OID specified in the sensor path and send only the requested traps. The job can remain in the Unknown state in these scenarios:

- If the collection job is invalid, the status of the job remains "Unknown."
- If configuration is missing on the device, the status of the job remains "Unknown."
- If no trap is received, the status of the job remains "Unknown."

For a list of supported traps and MIBs, refer to *List of pre-loaded traps and MIBs for SNMP collection*.

Table 26: List of Supported Non-Yang/OID based Traps

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

Sample payload of SNMP collection job

In this example, Crosswork sends an SNMP trap collection job to receive SNMP traps from network devices.

For detailed information about the API payload fields and usage examples, see the API documentation on Cisco Devnet.

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
```

```
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "TRAP_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "a9b8f43d-130b-4866-a26a-4d0f9e07562a",
            "8c4431a0-f21d-452d-95a8-84323a19e0d6",
            "eaab2647-2351-40ae-bf94-6e4a3d79af3a"
          ]
        }
      }
    },
    "sensor_input_configs": [
      {
        "sensor_data": {
          "trap_sensor": {
            "path": "1.3.6.1.6.3.1.1.4"
          }
        },
        "cadence_in_millisec": "60000"
      }
    ],
    "sensor_output_configs": [
      {
        "sensor_data": {
          "trap_sensor": {
            "path": "1.3.6.1.6.3.1.1.4"
          }
        },
        "destination": {
          "destination_id": "4c2ab662-2670-4b3c-b7d3-b94acba98c56",
          "context_id": "topic1_696600ae-80ee-4a02-96cb-3a01a2415324"
        }
      }
    ]
  }
}
```

Enabling trap forwarding with OID identification

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

These are the sample values used in the payload to forward traps to external applications:

- Link up

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4
  ```

- Link down

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3
  ```

- Syslog

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.9.9.41.2.0.1
  ```

- Cold start

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1
  ```

Sample payload to forward traps to 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"
    }
```

```
    ]
}
```

Syslog collection jobs

A Syslog collection job is a data collection process that

- uses Embedded Collectors to gather Syslog-based events from network devices in RFC 5424 and RFC 3164 formats
- employs SyslogSensors to filter events based on severity, facility, and regular expressions, and
- applies logical operators to customize filtering, reducing noise and optimizing the volume of collected Syslog data.

Supported Syslog formats

Embedded Collectors support the collection of Syslog-based events from network devices. The collectors support these Syslog message formats:

- RFC 5424
- RFC 3164

The supported Syslog formats are:

- RFC5424 Syslog format
- RFC3164 Syslog format

Filtering the Syslog events

A Syslog event filter is a configuration mechanism that:

- manages and controls the volume of Syslog data collected from devices through SyslogSensors
- supports PRI-based and filter-based rules that help capture relevant Syslog events for network monitoring and analysis, and
- applies filters based on severity, facility, or regular expressions to forward only required events, thereby reducing noise, optimizing storage, and streamlining downstream processing.

Syslog filters allow the use of logical operators such as `AND` and `OR` to define up to three filter combinations. This approach provides flexibility in how filters are evaluated.

Configure syslog data collection for Embedded Collectors

Enable syslog data collection from network devices using Embedded Collectors.

Use this procedure to configure the Embedded Collectors to receive syslog event data and forward it for monitoring and analysis with Crosswork.

Before you begin

Confirm the devices to be monitored are reachable and support the necessary capabilities.

Use these steps to configure syslog data collection.

Procedure

Step 1 Install the Element Management Functions application and configure the host information for syslog. For additional details, refer to the *Cisco Crosswork Network Controller 7.2 Installation Guide*.

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

Step 3 Configure the required parameters to enable syslog data collection from Embedded Collectors.

Note
The order of the steps does not affect the outcome. However, steps 2 and 3 are required; skipping either will prevent syslog data collection.

Additional information:

- For example configurations, refer to
  - Sample syslog configuration for single VM deployment
  - Sample device configuration for single VM deployment
- Review your platform-specific documentation to obtain configuration guidance.

Syslog data from selected devices is collected and made available in Crosswork via the Embedded Collectors.

Sample syslog collection payload

In this example, Crosswork sends a syslog-trap collection job to receive syslog messages sent from network devices. For detailed information about the API payload fields and usage examples, see the API documentation on Cisco Devnet.

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

Syslog collection jobs

A Syslog collection job is a data collection process that

- uses Embedded Collectors to gather Syslog-based events from network devices in RFC 5424 and RFC 3164 formats
- employs SyslogSensors to filter events based on severity, facility, and regular expressions, and
- applies logical operators to customize filtering, reducing noise and optimizing the volume of collected Syslog data.

Supported Syslog formats

Embedded Collectors support the collection of Syslog-based events from network devices. The collectors support these Syslog message formats:

- RFC 5424
- RFC 3164

The supported Syslog formats are:

- RFC5424 Syslog format
- RFC3164 Syslog format

Syslog collection job outputs

A Syslog collection job output is a record generated by the Syslog collector that:

- reflects the format configuration for the onboarded device
- contains Syslog events received from the device in the specified format, and

- is used to monitor and audit Syslog messages in Crosswork Network Controller.

When onboarding a network device, you must select the appropriate Syslog Format. The chosen format determines whether Syslog events are parsed and displayed as UNKNOWN, RFC5424, or RFC3164.

Syslog collection job output formats (Reference)

1. UNKNOWN: Syslog Collection Job output contains Syslog events as received from device.

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

Sample output:

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

```
}
version: "1"
```

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

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

RFC5424

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

Sample output:

```
....
....


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

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

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

RFC3164

"^(<(?<pri>\\d+)>[:]*\\s*)?(?<date>(*[a-zA-Z]{3}\\s+\\d+\\s+[0-9]{4}\\s+\\d+:\\d+:\\d+\\.[\\d{3}\\s+]+[[a-zA-Z]{3}[:]*]?\\s+)|(([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
}
....
....
```

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

Device configuration for non-secure Syslog

This section presents configurations for non-secure Syslog operation in Cisco IOS XR and IOS XE platforms, supporting both RFC3164 and RFC5424 message formats. Use the configurations below to achieve correct syslog parsing and message delivery.

Configure RFC3164 syslog format

For IOS XR:

```
logging <Data IP> port 30514 OR logging <Data IP> vrf <vrfname> port 30514
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>
```

Note Ensure “service timestamps log…” and “logging hostnameprefix…” are present.

For IOS XE:

```
no logging message-counter syslog
logging trap <severity>
logging facility <facility>
logging host <Data IP> transport tcp port 309898 session-id string <sessionidstring> -->
To use TCP channel
OR
logging host <Data IP> transport udp port 30514 session-id string <sessionidstring> --->
To use UDP channel
OR
logging host <Data IP> vrf Mgmt-intf transport udp port 30514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
```

Note TCP transports require explicit configuration as shown.

Configure RFC5424 syslog format

For IOS XR:

```
logging <Data IP> port 30514 OR logging <server 1> vrf <vrfname> port 30514
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
```

Note Ensure “service timestamps log…” and “logging hostnameprefix…” are present.

For IOS XE:

```
no logging message-counter syslog
logging trap <severity>
logging facility <facility>
logging host <Data IP> transport tcp port 309898 session-id string <sessionidstring> -->
To use TCP channel
OR
logging host <Data IP> transport udp port 30514 session-id string <sessionidstring> --->
To use UDP channel
OR
```

```
logging host <Data IP> vrf Mgmt-intf transport udp port 30514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
logging trap syslog-format 5424 --> if applicable
```

Note TCP transports require explicit configuration as shown.

Device configuration for secure Syslog

This section presents configurations for secure Syslog operation in Cisco IOS XR and IOS XE platforms, supporting both RFC3164 and RFC5424 message formats. Use the configurations below to achieve correct syslog parsing and message delivery.

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

- Download the Cisco Crosswork trust chain from the **Certificate Management UI** page in Cisco Crosswork. See Download syslog certificates, on page 208.
- Configure the device with the Cisco Crosswork trustchain. See Configure a Crosswork trustpoint on a device, on page 208.

Download syslog certificates

Provide users with the ability to download syslog certificates from the Crosswork Network Controller UI.

This task helps administrators securely export device syslog certificates for system integration, troubleshooting, or compliance requirements.

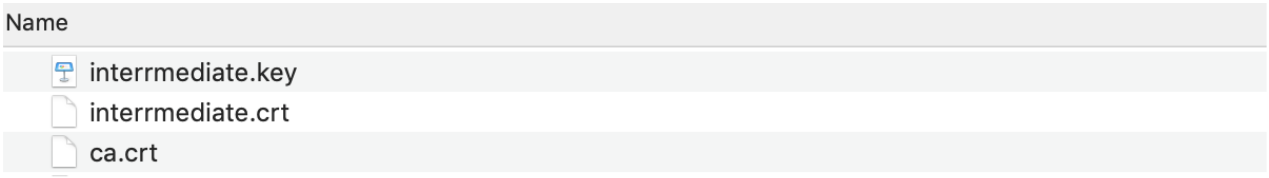
Procedure

Step 1 In the Crosswork Network Controller UI, go to **Administration > Certificate Management**.

Step 2 Click the *i* icon in the Crosswork-Device-Syslog row.

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

The files are downloaded to your system.



The files are downloaded to your system.

Configure a Crosswork trustpoint on a device

This procedure enables secure, trusted communication (TLS/PKI) between a Cisco device (IOS XR or IOS XE) and Crosswork applications using trustpoints.

When integrating network devices with Cisco Crosswork monitoring for authenticated, encrypted syslog export.

Procedure

Step 1 Enable TLS by configuring the IOS XR or XE device (refer to these samples):

- For IOS XR:

```
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 <Device Southbound IP>
!
logging trap debugging
logging format rfc5424
```

```
logging facility user
logging hostnameprefix ASR9k
logging suppress duplicates

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

- For IOS XE:

```
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 <Device Southbound IP> transport tls port 30614
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
```

Step 2 If configuring for FQDN, perform these additional steps:

a) Configure the domain name and DNS IP on the device:

- For IOS XR:

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

- For IOS XE:

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

b) Configure Embedded Collectors 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 <Device VIP FQDN>
```

- For IOS XE:

```
Device(config)# logging host fqdn ipv4 <hostname> transport tls port 30614
```

The device is now securely configured with a Crosswork trustpoint, enabling authenticated and encrypted log exports using TLS.

gNMI collection jobs

A gNMI telemetry collection is a data collection mechanism that:

- uses the gRPC Network Management Interface (gNMI) protocol via Embedded Collectors to gather telemetry data from devices
- supports only the gNMI Dial-In (gRPC Dial-In) streaming telemetry model based on subscriptions, relays subscription responses (notifications) to designated destinations, and
- relies on model compatibility with the target device platform. Devices require gNMI configuration before collection jobs can be initiated.

In the gNMI operation, Crosswork Network Controller can use both secure and insecure connection modes, with preference dictated by inventory settings. If a device reloads, the gNMI collector automatically resubscribes to maintain ongoing data collection. The gNMI specification does not define message termination, so some cadence controls are unsupported for gNMI collectors.

The gNMI specification does not define a message termination mechanism; therefore, Destination and Dispatch cadence settings are unsupported for gNMI collectors. The cadence parameter that controls polling frequency for Embedded Collectors is not applicable in gNMI-based collection.

Additional reference information

Supported gNMI subscribtion options

Embedded Collectors support multiple subscription paths per device, allowing combinations of ON_CHANGE and ONCE collection jobs:

- ON_CHANGE: Collects and delivers data only when specified elements change.
- ONCE: Collects and sends a one-time snapshot of the current data for the specified path.
- SAMPLE (under STREAM): Collects data at specified intervals if the device supports cadence-based collection.
- TARGET_DEFINED: The device determines the mode for each path (SAMPLE or ON_CHANGE) according to its capabilities.

Table 27: gNMI subscription options

Type	Subtype	Description
Once		Collects and sends the current snapshot of the system configuration only once for all specified paths.
Stream	SAMPLE	Cadence-based collection.
	ON_CHANGE	Sends initial state, then updates when the subscribed data changes.
	TARGET_DEFINED	Router or device selects mode (SAMPLE or ON_CHANGE) per path according to device configuration. Router/Device chooses the mode of subscription on a per-leaf basis based on the subscribed path (i.e. one of SAMPLE or ON_CHANGE)

Note

- Embedded Collectors depend on the device to declare supported subscription modes.
- gNMI sensor paths with default values do not appear in the payload due to Protocol Buffers conventions (e.g., default bool is false).

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

  Example:

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

  Example:

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

Sample gNMI collection payload

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

```
{
    "collection_job": {
        "job_device_set": {
            "device_set": {
                "device_group": "milpitas"
            }
        },
        "sensor_output_configs": [{
            "sensor_data": {
                "gnmi_standard_sensor": {
                    "Subscribe_request": {
                        "subscribe": {
                            "subscription": [{
                                "path": {
                                    "origin": "openconfig-interfaces",
                                    "elem": [{
                                        "name": "interfaces/interface/state/ifindex"
                                    }]
                                },
                                "mode": "SAMPLE",
                                "sample_interval": 10000000000
                            }, {
                                "path": {
                                    "origin": "openconfig-interfaces",
                                    "elem": [{
                                        "name":
"interfaces/interfaces/state/counters/out-octets"
                                    }]
                                },
                                "mode": "ON_CHANGE",
                                "sample_interval": 10000000000
```

```
                                }],
                                "mode": "STREAM",
                                "encoding": "JSON"
                            }
                        }
                    },
                    "destination": {
                        "context_id": "hukarz",
                        "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
                    }
                }],
                "sensor_input_configs": [{
                    "sensor_data": {
                        "gnmi_standard_sensor": {
                            "Subscribe_request": {
                                "subscribe": {
                                    "subscription": [{
                                        "path": {
                                            "origin": "openconfig-interfaces",
                                            "elem": [{
                                                "name": "interfaces/interface/state/ifindex"
                                            }]
                                        },
                                        "mode": "SAMPLE",
                                        "sample_interval": 10000000000
                                    }, {
                                        "path": {
                                            "origin": "openconfig-interfaces",
                                            "elem": [{
                                                "name":
"interfaces/interfaces/state/counters/out-octets"
                                            }]
                                        },
                                        "mode": "ON_CHANGE",
                                        "sample_interval": 10000000000
                                    }],
                                    "mode": "STREAM",
                                    "encoding": "JSON"
                                }
                            }
                        }
                    },
                    "cadence_in_millisec": "60000"
                }],
                "application_context": {
                    "context_id": "testing.group.gnmi.subscription.onchange",
                    "application_id": "testing.postman.gnmi.standard.persistent"
                },
                "collection_mode": {
                    "lifetime_type": "APPLICATION_MANAGED",
                    "collector_type": "GNMI_COLLECTOR"
                }
            }
        }
```

Enable secure gNMI communication between a device and Crosswork

Enable secure gNMI data exchanges between a device and Cisco Crosswork using certificate-based authentication.

Cisco Crosswork accepts a single rootCA for signing device certificates. All device certificates must be signed by the same CA, ensuring trusted and secure communication.

Before you begin

Ensure you have required certificate files (root CA, device certificates, device key).

Use these steps to enable secure gNMI between Cisco Crosswork and the devices.

Procedure

Step 1 Generate certificates for the device, signed by the rootCA trusted by Crosswork. See Generate the device certificates, on page 216.

Step 2 Upload the certificates to the Crosswork Certificate Management UI. See Configure the gNMI certificate, on page 218.

Step 3 Update device configuration with secure gNMI port details provided by Crosswork. See Update protocol on device from Crosswork, on page 151.

Step 4 Enable gNMI on the device. See Configure devices for gNMI-based telemetry, on page 219.

Step 5 Enable gNMI bundling on the device. See Configure gNMI bundling for IOS XR, on page 222.

Step 6 Configure the certificates and device key on the device. See Certificate management for IOS XR and XE devices, on page 223.

The device and Cisco Crosswork establish a secure, certificate-authenticated gNMI connection.

Generate the device certificates

Generate device certificates using OpenSSL for secure communication between devices and certificate authorities.

The certificate generation procedure has been validated using both OpenSSL and Microsoft tools. Contact Cisco Support if using a different tool.

Note To generate device certificates using a different utility, contact the Cisco Support team.

Before you begin

- Install OpenSSL on your system.
- Ensure you have access permissions for certificate storage.

Procedure

Step 1 Create the rootCA certificate.

a) Set the desired validity duration of the certificates using the “days” parameter (recommended: 365 or more).

```
# 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
```

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
```

a) For multiple devices, specify multiple IP addresses in the subjectAltName, separated by commas in `subjectAltName`.

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

Step 3 Verify the certificate contains the expected Subject Alternative Name (SAN) details.

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

The system generates a device certificate with the designated subject alternative names, enabling secure communication.

Sample output:

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

```
bc:c6:a0:31:7c:1f:d7:5e:c6:86:72:43:a8:c1:0c:70:33:60:
dc:14:5b:9d:f3:ab:3d:d5:d2:94:90:1c:ba:fd:80:4d:22:e3:
31:93:c7:16:5f:85:20:38:ad:36:b9:1a:e0:89:8e:06:8c:f8:
cd:55:cc:a1:89:d3:91:7f:66:61:a3:40:71:c2:1e:ee:3b:80:
37:af:73:5e:8e:0d:db:4b:49:da:a6:bd:7d:0a:aa:9e:9a:9e:
fa:ed:05:25:08:f2:4d:cd:2f:63:55:cf:be:b1:5d:03:c2:b3:
32:bf:f4:7b:1a:10:b9:5e:69:ac:77:5e:4a:4f:85:e3:7f:fe:
04:df:ce:3e:bb:28:8f:e3:bf:1a:f9:0f:94:18:08:86:7d:59:
57:71:0a:97:0d:86:9c:63:e7:0e:48:7d:f0:0e:1d:67:ff:9b:
1d:1b:05:25:c8:c3:1f:f4:52:0f:e1:bf:86:d7:ec:47:10:bd:
94:cf:ca:e2
```

Configure the gNMI certificate

Upload and configure a gNMI certificate in Cisco Crosswork to enable secure device communication via gNMI.

gNMI collectors operate as clients and access devices (gNMI servers). They require a valid certificate for trust validation. The certificate establishes a trusted chain for device authentication.

Before you begin

- Ensure you have the root CA (.pem) or relevant trust chain file available.
- Gather the necessary certificate details (such as name and role).
- Verify that the trust chain in your .pem file includes all devices participating in gNMI communication.
- Be aware that you can upload only one gNMI certificate to Crosswork.

Procedure

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

Step 2 Click the + icon to add the certificate.

Step 3 In the **Add Certificate** window, provide these details:

a) **Device Certificate Name**: Enter a name for the certificate.
b) Certificate Role: Select "Device gNMI/gRPC communication".
c) Device Trust Chain: Upload the Root CA file or trust chain (.pem file).

If you have multiple trust chains, add all of them (across vendors) to a single .pem file and upload that.

Step 4 Click **Save**.

The newly added gNMI certificate appears in the configured certificates list.

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 devices for gNMI-based telemetry

This section provides instruction on how to enable both platforms to collect and export telemetry data using gNMI.

Enable gNMI-based telemetry data collection on IOS XR and IOS XE devices.

- On Cisco IOS XR devices, enable the gNMI service and specify telemetry parameters. See Configure IOS XR device for gNMI, on page 219.
- On Cisco IOS XE devices, enable gNMI and configure required access credentials. See Configure IOS XE device for gNMI, on page 221.

Configure IOS XR device for gNMI

Configure IOS XR devices to enable gNMI-based telemetry data collection.

Use these instructions to enable gNMI on IOS XR devices so telemetry collectors can stream data via gRPC over HTTP/2.

Before you begin

- Confirm the network environment supports gRPC over HTTP/2.
- Obtain any necessary port numbers and security certificates.

Procedure

Step 1 Enable gRPC on an HTTP/2 connection.

a) Enter configuration mode and activate gRPC with a specified port:

Example:

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

b) Specify a port number within the range 57344 to 57999. If the port number is unavailable, an error will appear.

Step 2 Configure session parameters.

where:

a) Use this command structure:

Example:

```
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 }
```

b) Parameter options:

Table 28: Parameters and descriptions

Parameters	Descriptions
`address-family`	Set the address-family identifier type.
`dscp`	Set the DSCP QoS marking on transmitted gRPC traffic.
`max-request-per-user`	Set the maximum concurrent requests per user.
`max-request-per-user`	Set the maximum concurrent requests per user.
`max-request-total`	Set the maximum concurrent requests in total.
`max-streams`	Set the maximum number of concurrent gRPC requests. The maximum subscription limit is 128 requests. The default is 32 requests.
`max-streams-per-user`	Set the maximum concurrent gRPC requests for each user. The maximum subscription limit is 128 requests. The default is 32 requests.
`no-tls`	Disable transport layer security (TLS). TLS is enabled by default.
`service-layer`	Enable gRPC service layer configuration.
`tls-cipher`	Enable gRPC TLS cipher suites.
`tls-mutual`	Enable mutual authentication.

Parameters	Descriptions
`tls-trustpoint`	Configure trustpoint.
`server-vrf`	Enable server VRF.

Step 3 Enable Traffic Protection for Third-Party Applications (TPA) on the device.

a) Configure the following settings:

Example:

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

The IOS XR device is configured to support secure, scalable, gNMI-based telemetry streaming as required for modern network data collection.

Configure IOS XE device for gNMI

Configure IOS XE devices to enable gNMI-based telemetry data collection.

Use these instructions to enable gNMI on IOS XE devices so telemetry collectors can stream data via gRPC over HTTP/2.

Before you begin

- Confirm that your network environment supports gRPC over HTTP/2.
- Obtain required port numbers for gNMI telemetry.
- Acquire security certificates if you are enabling secure gNMI.

Procedure

Step 1 Access device CLI in global configuration mode.

Step 2 Enable the gNMI server in the insecure mode.

Example:

```
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
```

Step 3 Enable the gNMI server in the secure mode.

Example:

```
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
```

The IOS XE device is now configured to stream telemetry data using gNMI over gRPC/HTTP2. Telemetry collectors can connect using the configured insecure or secure port.

What to do next

Validate the gNMI connection from your telemetry collector.

Configure gNMI bundling for IOS XR

Enable and configure gNMI bundling capability to optimize telemetry updates on IOS XR devices.

gNMI bundling allows IOS XR to combine multiple Update messages into a single Notification message within a SubscribeResponse. This improves efficiency by reducing the number of notifications sent. You must enable bundling and specify the message size on the IOS XR device.

Before you begin

The gNMI bundling capability can only be configured from the device. It is not available in the Crosswork Interface. Details on how the bundling feature works are available in the Programmability Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.8.x.

Procedure

Step 1 Enable gNMI bundling:

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

Note
The gNMI bundling capability is disabled by default.

Step 2 Set the bundling size, as needed:

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

The default bundling size is 32768 bytes.

Note
After processing the (N - 1)th instance, if the message size is less than the configured bundling size, one more instance may be included. This may result in the bundling size being exceeded.

The IOS XR device transmits bundled Update messages according to the specified message size, optimizing telemetry update delivery.

What to do next

To verify bundling is enabled and configured, use:

```
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)
```

Certificate management for IOS XR and XE devices

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

Certificate management encompasses the procedures and requirements for securing communications between Cisco IOS XR and IOS XE devices:

- Cisco IOS XR: Requires certificate and trustpoint configuration for enabling secure gNMI. See Install certificates on a Cisco IOS XR device, on page 223.
- Cisco IOS XE: Similarly requires certificate and trustpoint setup for secure gNMI operations. See Install certificates on a Cisco IOS XE device, on page 224.

Install certificates on a Cisco IOS XR device

Import and install device certificates to enable secure gNMI server operation on Cisco IOS XR.

Certificates and a trustpoint are required only when configuring secure gNMI servers. This procedure guides you through all necessary installation steps.

Before you begin

- Ensure you have the following files ready: `rootCA.pem`, `device.key`, and `device.crt`.
- Ensure access to the IOS XR device filesystem.

Use these steps to install certificates on a Cisco IOS XR device.

Procedure

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

Step 2 Log in to the IOS XR device.

Step 3 Enter the VM shell mode.

Example:

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

Step 4 Navigate to the `/grpc` directory.

Example:

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

Step 5 Create or replace the contents of these files in `/misc/config/grpc`.

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

a) If enabling TLS for the first time, copy the following from `/tmp`:

- ems.pem with device.crt
- ems.key with device.key
- ca.cert with rootCA.pem

b) If TLS was previously enabled, overwrite these files with the new content.

Step 6 Restart TLS on the device to activate changes:

a) Disable TLS with the `no-tls` command.
b) Re-enable TLS with the `no no-tls` configuration command.

Device certificates are installed, and TLS is restarted. The IOS XR device is ready for secure gNMI operations.

Install certificates on a Cisco IOS XE device

Enable secure gNMI server operation on a Cisco IOS XE device by installing the required certificates and configuring a trustpoint.

Certificates and a trustpoint are required only when configuring secure gNMI servers. This procedure guides you through all necessary installation steps.

Before you begin

- Plan and note the trustpoint name and password you will use.

  Obtain these files:

  - The root CA certificate (e.g., rootCA.pem)
  - The device’s encrypted private key (e.g., device.des3.key)
  - The device certificate (e.g., device.crt)

Procedure

Step 1 Enter global configuration mode.

Step 2 Import the root CA certificate using the `crypto pki import [trustpoint] pem terminal password [password]` command.
When prompted, paste the contents of your rootCA.pem file, followed by "quit" on a new line.

Step 3 When prompted, import the device's encrypted private key.

a) Paste contents, a by "quit", as instructed.

Step 4 When prompted, import the device certificate.

a) Paste contents, followed by "quit," as instructed.

Step 5 Configure trustpoint parameters as needed (such as revocation checks).

Example:

```
# 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#
```

The certificates and key are installed, enabling secure gNMI server operation on Cisco IOS XE.

Collection job status fields and interpretations

Collection job status provides detailed information regarding each active collection job across all Embedded Collector instances registered to Cisco Crosswork.

View active collection jobs

You can monitor the status of collection jobs that are currently active on all Embedded Collector instances enrolled with Crosswork Network Controller from the Collection Jobs page. The left pane lists all active collection jobs and displays their Status, App ID, Context ID, and Action. Use the Action drop-down to delete collection jobs or refresh the status of a collection job and its associated tasks.

The **Job Details** pane shows the details of all collection tasks that are associated with a particular job in the left pane. The overall status of the Collection job in the **Collection Jobs** pane is the aggregate status of all the collection tasks in the **Jobs Details** pane.

View job details

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

- Application name and context associated with the collection job
- Collection job status
- Job configuration of the collection job that you pass in the REST API request. Click the icon next to Config Details to view the job configuration. Crosswork Network Controller lets you view configuration in two modes:
  - View Mode
  - Text Mode
- Collection type
- Last modified date and time
- Collections (x): Number of input collections; Issues (y) shows how many are UNKNOWN or FAILED
- Distributions (x): Number of output collections; Issues (y) shows how many are UNKNOWN or FAILED

The overall job status is based on the aggregate status of all related collection tasks.

Key parameters shown for collection jobs

The Collection Jobs and Job Details panes display these information for active collection jobs:

Table 29: Collection jobs fields and descriptions

Field	Description
Collection/Distribution Status	Current status of the collection/distribution; updated on change. Click icon for details.

Field	Description
Hostname	Device hostname for the collection job.
Device Id	Unique identifier of the device being monitored.
Sensor Data	The sensor paths involved; view metrics summary for cadence-based statistics. 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 a cadence-basis, i.e., once every 10 minutes by default. It shows the following metrics for a collection: • last_collection_time_msec • total_collection_message_count • last_device_latency_msec • last_collection_cadence_msec It shows the following metrics for a collection: • total_output_message_count • last_destination_latency_msec • last_output_cadence_msec • last_output_time_msec • total_output_bytes_count
Destination	Data destination for the job.
Last Status Change Reported Time	Time and date of the last status change was reported for the device sensor pair.

Guidelines for interpreting the collection job states

- The status of a collection task associated with a device after it is attached to an Embedded Collector, is **Unknown**.
- A job could have status as **Unknown** for one of the following reasons:
  - Embedded Collectors have not yet reported its status.
  - Loss of connection between Embedded Collectors and Cisco Crosswork.
  - Embedded Collectors have received the collection job, but the actual collection is still pending. For example, traps are not being sent to Embedded Collectors southbound interface, or the device is not sending telemetry updates.

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

- After the collection job is processed, the status changes to 'Successful' if the processing was successful or else it changes to 'Failed'.
- If a collection job is in a degraded state, one of the reasons might be that the static routes to the device have been erased from Embedded Collectors.
- Collections to a destination that is in an Error state do not stop. The destination state is identified in the background. If the destination is in an Error state, the error count is incremented. Drill down on the error message that is displayed in the **Distribution** status to identify and resolve the issue by looking at respective collector logs.
- Cisco Crosswork Health Insights - KPI jobs must be enabled only on devices mapped to an extended Embedded Collector instance. Enabling KPI jobs on devices that are mapped to a standard Embedded Collector instance reports the collection job status as **Degraded** and the collection task status as **Failed** in the **Jobs Details** pane.

Create a collection job

You can publish collection jobs created through the Crosswork Network Controller UI page only once.

Use the Crosswork Network Controller UI to create jobs that collect device or network data via CLI or SNMP. These jobs enable centralized data collection for analysis or export.

Before you begin

Ensure that a data destination is created and active for depositing collected data. Make sure you have the details of the sensor path and MIB from which you plan to collect data.

Procedure

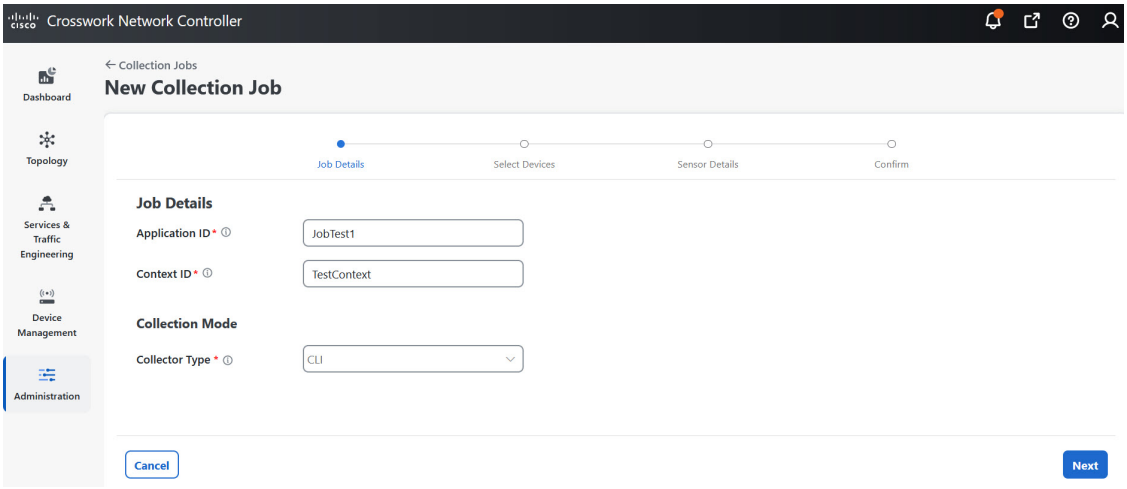
Step 1 Go to **Administration > Data Gateway Management > Collection Jobs > Bulk Jobs**.

Step 2 Click  .

Step 3 On the **Job details** page, enter values for these fields:

- **Application ID**: A unique identifier for the application.
- **Context**: A unique identifier to identify your application subscription across all collection jobs.
- **Collector Type**: Select the type of collection as either CLI or SNMP.

Figure 53: Job details



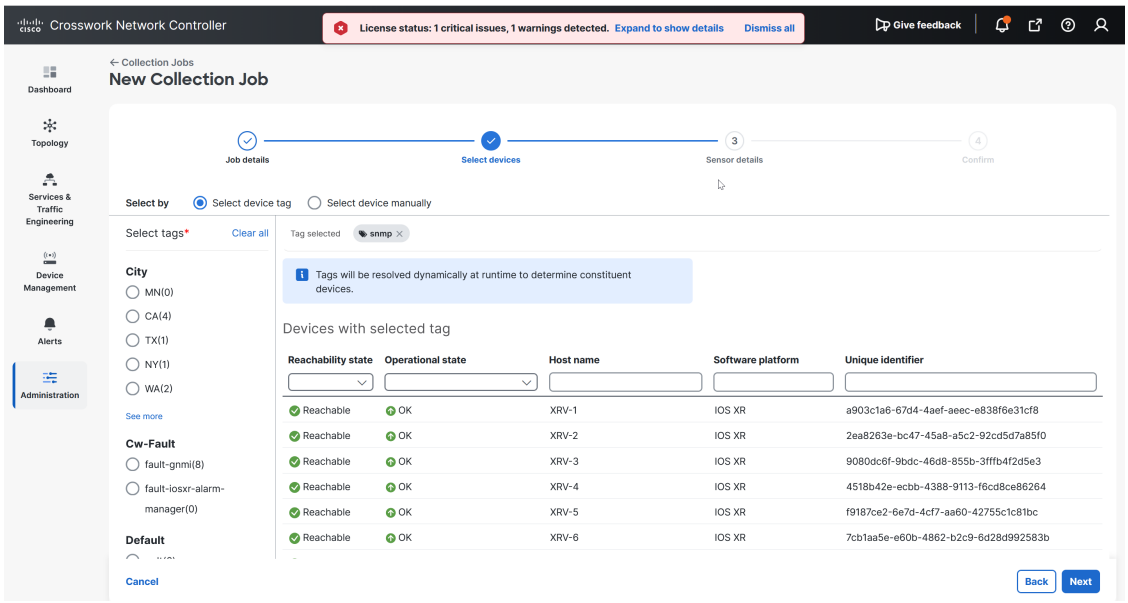
a) Click **Next**.

Step 4 Select the devices from which you want to collect data.

You can select devices by device tag or choose them manually.

a) Click **Next**.

Figure 54: Select devices



Step 5 Enter these sensor details for CLI collection:

a) Select data destination from the **Select Data Destination** drop-down list.

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

c) If you select **CLI PATH**, click + and enter these parameters in the **Add CLI Path** dialog box:

- **Collection Cadence**: Push or poll cadence in seconds

- **Command**: CLI command
- **Topic**: Topic associated with the output destination

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

d) If you select **Device Package**, click + and enter these parameters in the **Add Device Package Sensor** dialog box:

- **Collection cadence**: Push or poll cadence in seconds
- **Device Package Name**: Custom XDE device package ID used when creating the device package
- **Function name**: Function name within custom XDE device package
- **Topic**: Topic associated with the output destination

e) Enter Key and String value for the parameters.
f) Click **Save**.

Figure 55: Sensor details for CLI path

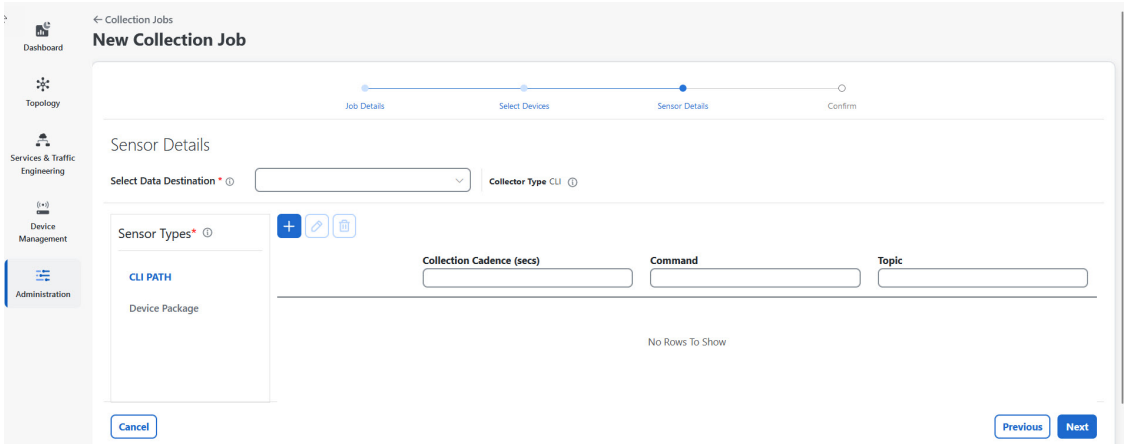


Figure 56: Add CLI path

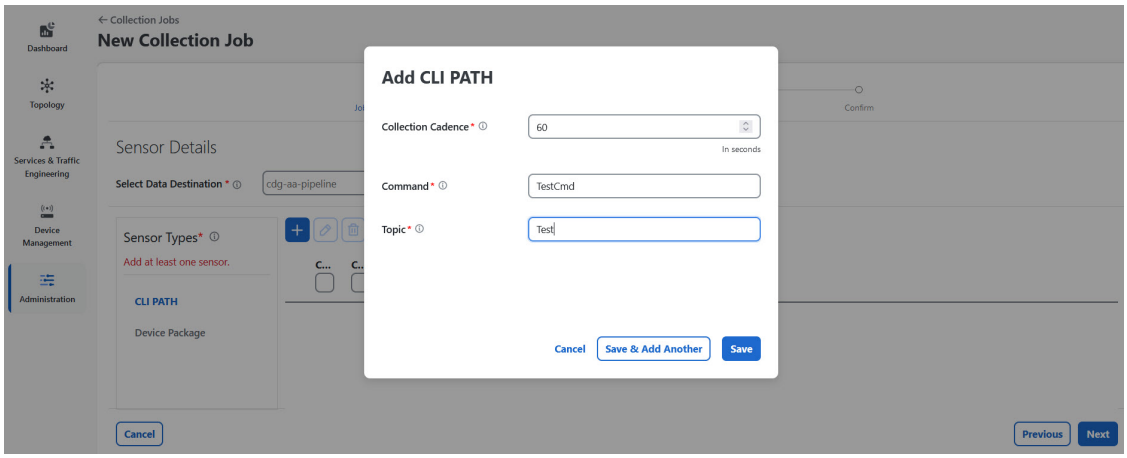
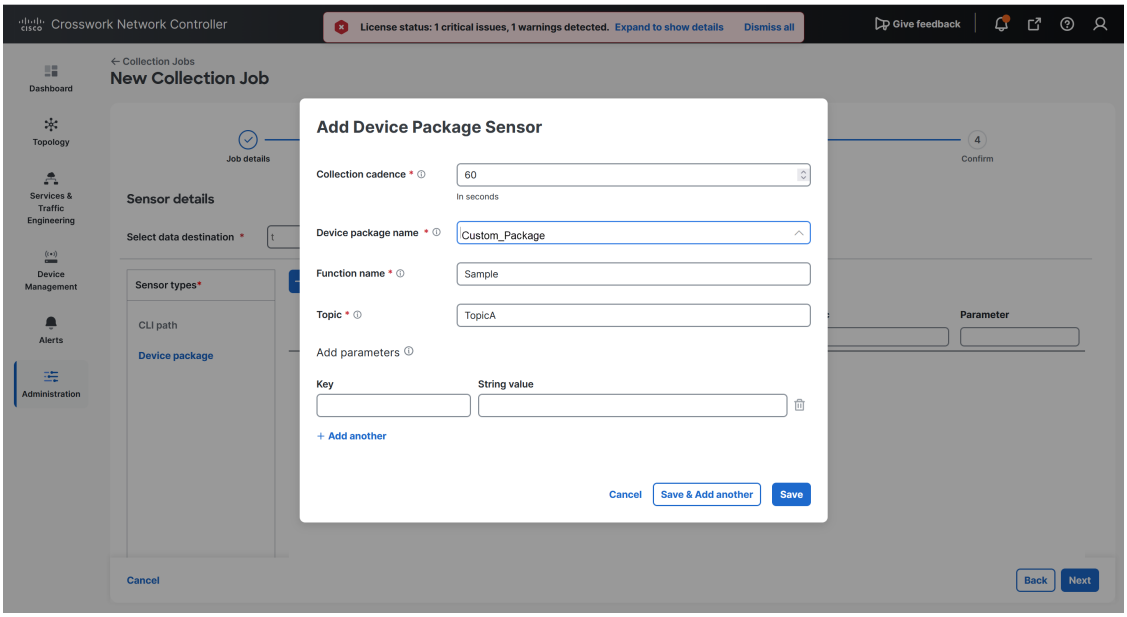


Figure 57: Add device package sensor



Step 6 Enter these sensor details for SNMP collection:

a) Select data destination from the **Select Data Destination** drop-down list.

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

c) If you select **SNMP MIB**, click + and enter these parameters in the **Add Device Package Sensor** dialog box:

- **Collection Cadence**: Push or poll cadence in seconds.
- **OID**
- **Operation**: Select the operation from the list.
- **Topic**: Topic associated with the output destination.

d) If you select **Device Package**, click + and enter values for these parameters in the Add Device Package Sensor dialog box:

- **Collection Cadence**: Push or poll cadence in seconds.
- **Device Package Name**: Custom device package ID used when creating the device package.
- **Function name**: Function name within custom device package.
- **Topic**: Topic associated with the output destination.

e) Enter the key and string value for the parameters.

f) Click **Save**.

Figure 58: Sensor details for SNMP path

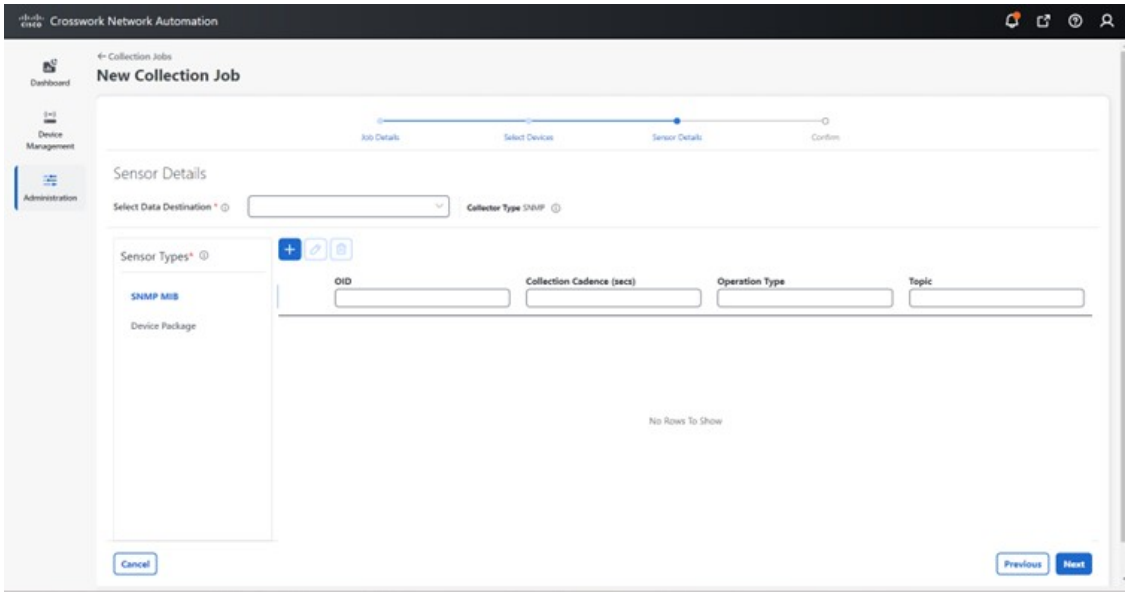
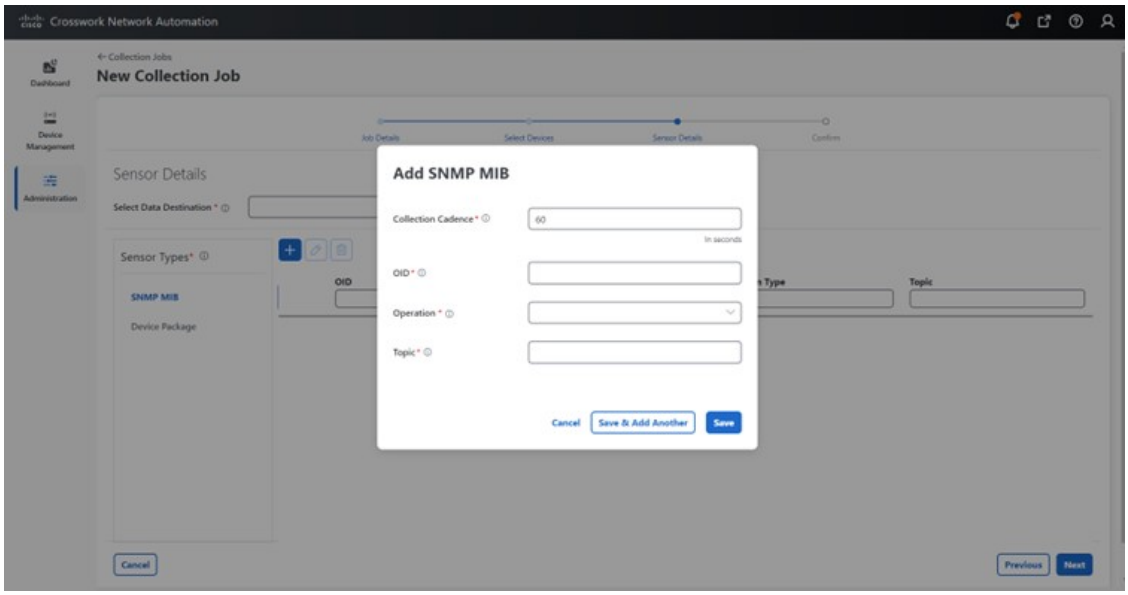


Figure 59: Add SNMP MIB



Step 7 Click **Create Collection Job**.

The new collection job is published and starts gathering data according to configuration.

What to do next

Review job status and ensure data is being deposited to the specified destination as expected.

View active collection jobs

View all currently active collection jobs on Embedded Collector instances.

Use the **Collection Jobs** page in Cisco Crosswork to get an overview of every active collection job and interact with status and management controls.

Procedure

Step 1 Go to the **Collection Jobs** page in the Crosswork Network Controller UI.

Step 2 From the left navigation bar, choose **Administration > Collection Jobs**.

Step 3 Review the list of active collection jobs and note their Status, App ID, Context ID, and Action.

Step 4 Use the **Action** drop-down to delete a collection job or refresh the status of a job and its associated tasks.

You can view the real-time status of active collection jobs and manage them for all enrolled Embedded Collector instances.

Delete a collection job

Remove an unwanted external collection job from your system.

Deleting a collection job also deletes its associated collection tasks. Delete jobs created by Health Insights by disabling the KPI profile. This action removes the collection jobs that the profile deployed.

Before you begin

Do not delete system jobs created by Crosswork Applications as deletion could cause collection issues.

Jobs created by Health Insights should only be deleted by disabling the KPI profile which will remove the collection jobs it deployed.

Procedure

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

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

Step 3 Select the collection job you want to delete.

Step 4 In the job's row, select **Delete**.

Step 5 Confirm by clicking **Delete** in the confirmation window.

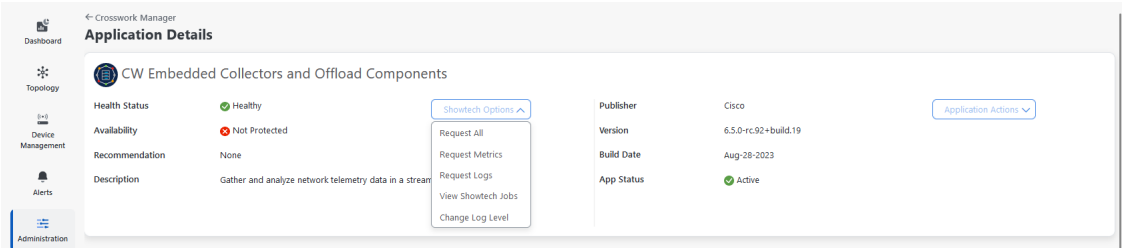
The selected collection job and its collection tasks are deleted.

Check the health status of Embedded Collectors

View the operational health and status of all embedded collectors in Cisco Crosswork.

The CW Embedded Collectors and Offload Components tile provides the operations and health summary of Embedded Collectors. You can find information about the health of pods running on the Crosswork container on this page. The overall health of the Embedded Collectors application depends on the health of each individual pod service.

Figure 60: Crosswork Embedded Collector and Offload Component



Procedure

Step 1 From the main menu, choose **Administration > Crosswork Manager > CW Embedded Collectors and Offload Components**.
You can see the health and status summary of embedded collectors, along with detailed pod health information, in the displayed pane.

Step 2 Optionally, use the **Showtech Options** drop-down to:

- **Request All**: Collects both logs and metrics for the embedded collectors. To view the logs, navigate to Crosswork Manager > Application Management > Showtech Requests.
- **Request Metrics**: Collects only metrics information.
- **Request Logs**: Collects only log information.
- **View Showtech Jobs**: Displays the progress and status of Showtech jobs. You can also see job details from Crosswork Manager > Application Management > Showtech Requests.
- **Change Log Level**: Changes the log level of selected Embedded Collector components, such as collectors (e.g., cli-collector) and infrastructure services (e.g., oam-manager). The change affects only the targeted collector.

Step 3 Optionally, use the **Application Actions** drop-down to:

- **Install**: Installs a new collector with profile, hostname, and management interface details from previous collectors.
- **Upgrade**: Upgrades the collector to a newer version.
- **Activate**: Activates selected collectors.
- **Uninstall**: Removes the collector application. Uninstalling the application may interrupt ongoing collection jobs and cause data loss for current operations.

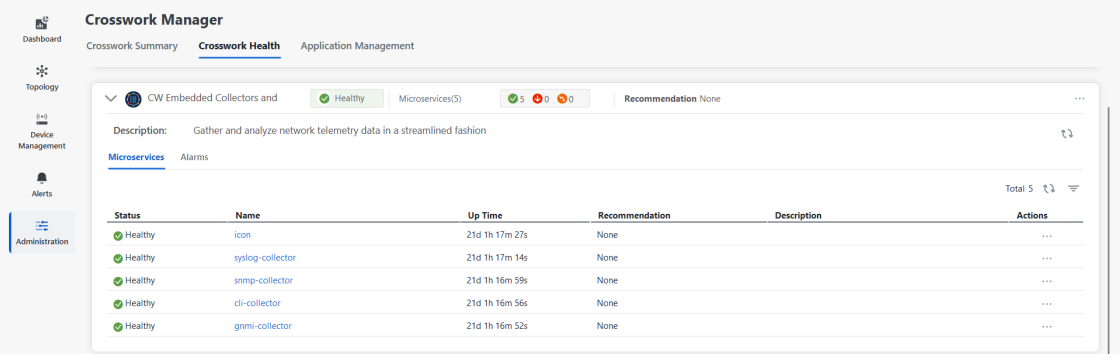
You have reviewed the current health status, accessed logs and metrics as needed, and can take corrective actions.

Monitor the collector's pod health

Ensure the health of the collector pod to maintain optimal collection performance. Take timely corrective action to prevent service disruption.

In the Embedded Collector and Offload Component pane, you can view a detailed overview of the health status of pods hosting collectors or microservices. We recommend regularly monitoring the health of the collector pods in your network. This helps avoid overloading and enables proactive corrective measures, such as adding more resources or reducing the load on the collector in a timely manner.

Figure 61: Microservices Tab



Procedure

Step 1 Go to **Administration > Crosswork Manager > CW Embedded Collectors and Offload Components**.

Step 2 Expand CW Embedded Collectors and Offload Components, then select **Microservices**.

Step 3 (Optional) In the **Microservices** tab, type the collector name in the **Name** field to locate the collector pod.

Step 4 (Optional) From this page, click  under the **Actions** column to perform these actions:

- **Restart**: restarts the collector pod. Restarting a pod disrupts the ongoing collection process. If you need to restart, start, or stop a process, we strongly advise consulting the Cisco TAC team.
- **Showtech Requests**: displays the showtech jobs executed for the corresponding collector pod. To view the logs, go to **Crosswork Manager > Application Management > Showtech Requests**.
- **Request All**: collects both logs and metrics of the pod. To view the logs, go to **Crosswork Manager > Application Management > Showtech Requests.**
- **Request Metrics**: collects the metrics of the pod.
- **Request Logs**: collects the logs of the pod.

View collector alarms and events

Enable users to monitor collector alarms and events to identify and remediate potential data collection issues.

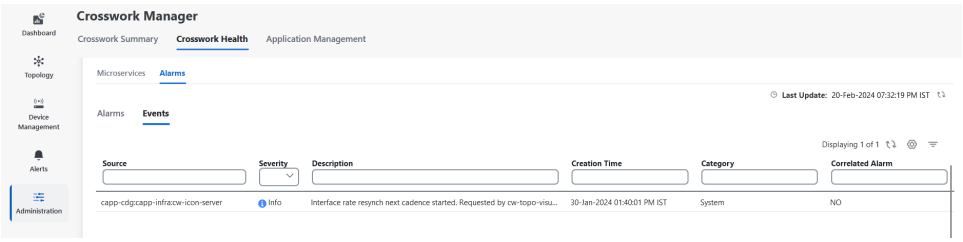
Embedded Collectors in the Crosswork Network Controller generate alarms when anomalies prevent data collection. By monitoring these alarms, you can detect issues that affect collector performance and take necessary action.

Procedure

Step 1 From the Crosswork Network Controller UI, go to **Administration > Crosswork Manager > CW Embedded Collectors and Offload Components**.

The **Alarms** tab provides a consolidated list of all collector alerts and events.

Figure 62: Events



Step 2 Toggle between the **Alarms** and **Events** subtabs to view the respective details.

Step 3 Filter the alarms or events list by:

- adjusting column filters,
- changing the **Active Alarms Only** slider, and
- adding or removing columns using the ⚙ icon.

You can view all current collector alarms and events. This enables timely detection and troubleshooting of potential data collection issues.

Embedded Collector troubleshooting scenarios

The troubleshooting section contains information about the possible issues and corrective actions that you may observe with Embedded Collectors.

Troubleshooting the admin state change from DOWN to UP

In a single VM deployment, devices are automatically attached to Embedded Collectors, which causes their Admin State to change from DOWN to UP.

Workaround: If you need to change the Admin State to DOWN, manually update it using the **Edit Device** page. For detailed steps on editing a device, see the **Edit Devices** section in the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management* guide.

Kafka connection failure for unsecured external destinations

If a collection job is submitted to an external (unsecured) Kafka destination, the dispatch job may fail to connect to the Kafka server.

Collector error:

```
org.apache.kafka.common.errors.TimeoutException: Topic cli-job-kafka-unsecure not present
in metadata after 60000 ms.
```

Kafka error:

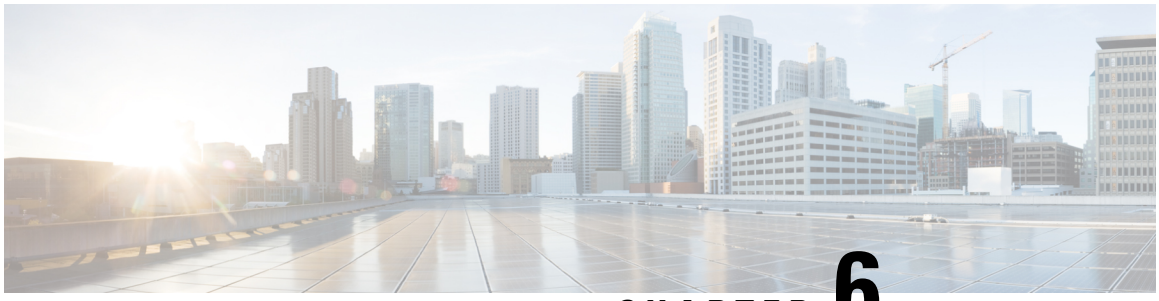
```
SSL authentication error "[2021-01-08 22:17:03,049] INFO [SocketServer brokerId=0] Failed
authentication with /80.80.80.108 (SSL handshake failed)
(org.apache.kafka.common.network.Selector).
```

These errors appear when the required port on the external Kafka VM is blocked, preventing the collector from connecting.

Workaround:

1. On the Kafka Docker host or server, run this command to verify whether the Kafka port is listening:

   ```
   netstat -tulpn
   ```
2. Unblock or correct the port configuration on the Kafka server. After fixing the issue, restart the Kafka server process to restore connectivity.



CHAPTER 6

Prepare Infrastructure for Device Management

This chapter provides an overview of key setup concepts—such as credential profiles, providers, and tags—and directs you to the relevant tasks and reference material needed to prepare your environment for comprehensive device management.

Manage credential profiles

A credential profile is a collection that

- stores credentials for various network protocols (such as SNMP, Telnet, SSH, and HTTP) set at the device level,
- enables consistent application of credentials when adding devices or providers, and
- automates device configuration changes, streamlines monitoring, and facilitates communication with providers.

Credential profiles may include as many protocols and their corresponding credentials as needed within a single profile. They must contain credentials that match those configured on devices.

Credential profiles page

From the **Credential profiles** page, you can create a new credential profile, update the settings configured for an existing profile, or delete a profile. To open this page, choose **Device Management** > **Credential profiles**.

Figure 63: Credentials profile page

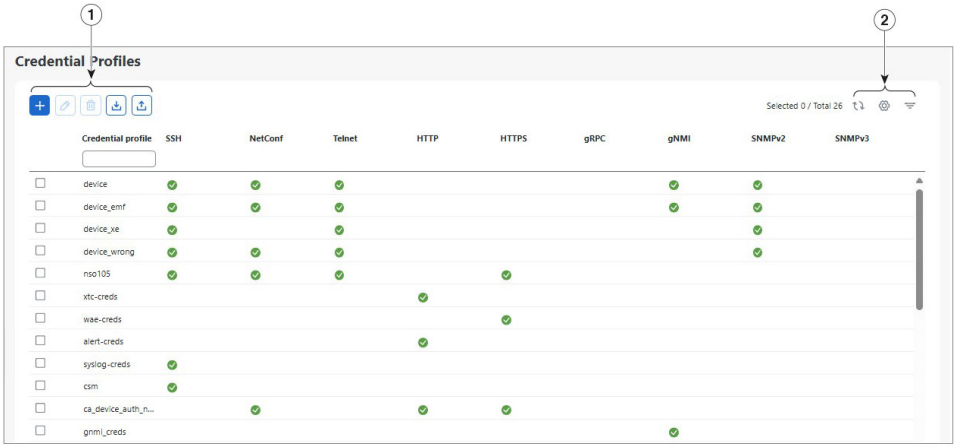


Table 30: Credentials profile page items

Item	Description
1	Click + to add a credential profile. See Create credential profiles, on page 240.
	Click edit to edit the settings for the selected credential profile. See Edit credential profiles, on page 244.
	Click delete to delete the selected credential profile. See Delete credential profiles, on page 245.
	Click import to import new credential profiles from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import credential profiles using a CSV file, on page 241.
	Click export to export credential profiles to a CSV file. See Export credential profiles, on page 245.
2	Click refresh to refresh the **Credential Profiles** window.
	Click settings to choose the columns to make visible in the **Credential Profiles** window.
	Click filter to set filter criteria on one or more columns in the **Credential Profiles** window.
	To clear a filter, click the corresponding [X] in the Filters menu.

Create credential profiles

This section explains how to create a new credential profile using the Crosswork Network Controller UI.

Note If you have many credential profiles to import, you may find it more efficient to put the information in a CSV file and import the file. Refer to Import credential profiles using a CSV file for instructions.

To create a new credential profile, complete these steps:

Procedure

Step 1 Choose **Device Management** > **Credential Profiles** > .

Step 2 Enter a descriptive profile name to ensure it is easily distinguishable from other credential profiles. The name can contain a maximum of 128 alphanumeric characters. You can use letters, numbers, dots (.), underscores (_), and hyphens (-).

Step 3 Select a protocol from the **Connectivity type** drop-down list. Confirm what connection types must be configured in a credential profile for specific providers. Refer to Provider families, on page 247 for a list of supported provider families.

Step 4 Complete the applicable credentials and ensure they match what is already on the device.

Step 5 To add more protocols, click **+ Add Another** and repeat the previous steps.

Step 6 Click **Save**.

Import credential profiles using a CSV file

If you need to add many credential profiles, add the information to a CSV file and import it. Importing credential profiles from a CSV file adds the profiles to the database. Any duplicate profiles that already exist are overwritten.

Additional security

To maintain network security, use asterisks instead of real passwords and community strings in any CSV file you plan to import. After the import, follow the steps in Edit credential profiles, on page 244 to replace the asterisks with actual passwords and community strings.

Considerations when replacing an existing CSV file

When you re-import a credential profile CSV file that you have exported and edited, all passwords and community strings in the exported file are replaced with asterisks (*). You cannot re-import an exported credential profile CSV file with blank passwords.

To import credential profiles using a CSV file, complete these steps:

Procedure

Step 1 Choose **Device Management** > **Credential Profiles** > .

Step 2 If you have not already created a credential profile CSV file to import:

a) Click the **Download sample 'Credential template (*.csv)' file** link and save the CSV file template to your local drive.

b) Open the template using your preferred tool and edit one row for each credential profile. See Credential profile template guidelines, on page 242.
c) When you are finished, save the new CSV file.

Step 3 Click **Browse** to navigate and open the CSV file.

Step 4 With the CSV file selected, click **Import**.

The credential profiles you imported should now be displayed in the **Credential Profiles** window.

Credential profile template guidelines

Use these guidelines when editing the credential template:

- Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. The order in which you enter values in each field is important because it determines how fields are mapped to each other. For example, if you enter **SSH**;**NETCONF**;**TELNET** in the **Connectivity Type** field and you enter **UserTom**;**UserDick**;**UserHarry**; in the **User Name** field, the entries are mapped in order.
  - SSH: UserTom
  - NETCONF: UserDick
  - TELNET: UserHarry
- Enter SNMP community string information exactly as currently entered on your devices. Failure to do so will result in loss of device connectivity, and inability to collect certain KPI data or execute configured Playbooks on devices associated with the credential profile.
- Password and community string information associated with a user ID are stored in plain text in the CSV file you prepare. Review the security implications of storing credentials and apply appropriate safeguards.
- Delete the sample data rows before saving the file. If you keep the sample rows, the imported data will include both sample and intended information. Column header rows are always ignored during import.
- Each row defines a credential profile. This table helps you populate each credential profile.

Table 31: Credential profile template guidelines

Field	Entries	Required or Optional
Credential Profile	The name of the credential profile. For example, **nso** or **srpce**.	Required

Field	Entries	Required or Optional
Connectivity Type	Valid values are SSH, SNMPv2, NETCONF, TELNET, HTTP, HTTPS, GNMI, SNMPv3, or TL1.	Required • Devices—SNMP and SSH are required to avoid operational errors due to clock synchronization checks. • SR-PCE—Since SR-PCE is considered a provider and a device, SSH, and HTTP are required. • NSO—NETCONF is required. **Note** SSH and SNMP credentials are mandatory for onboarding devices and synchronizing with the NSO provider.
User Name	For example, NSOUser	Required if **Connectivity Type** is **SSH**, **NETCONF**, **TELNET**, **HTTP**, **HTTPS**, **SNMPv3**, or **GRPC**.
Password	The password for the specified **User Name**.	Required
Enable Password	Use an Enable password. Valid values are: **ENABLE**, **DISABLE**, or leave blank (unselected)	Required if **Connectivity Type** is **SSH** or **TELNET**. Otherwise leave the field blank.
Enable Password Value	Specify the Enable password to use.	Required if **Connectivity Type** is **SSH** or **TELNET**, and **Enable Password** is set to **ENABLE**. Otherwise leave blank.
SNMPV2 Read Community	For example: **readprivate**	Required if **Connectivity Type** is **SNMPv2**
SNMPV2 Write Community	For example: **writeprivate**	Required if **Connectivity Type** is **SNMPv2**
SNMPV3 User Name	For example: **DemoUser**	Required if **Connectivity Type** is **SNMPv3**
SNMPV3 Security Level	Valid values are **noAuthNoPriv**, **AuthNoPriv** or **AuthPriv**	Required if **Connectivity Type** is **SNMPv3**

Field	Entries	Required or Optional
SNMPV3 Auth Type	Valid values are • HMAC_SHA2-512 • HMAC_SHA2_384 • HMAC_SHA2_256 • HMAC_SHA2_224 • HMAC_MD5 • HMAC_SHA	Required if **Connectivity Type** is **SNMPv3** and **SnmpV3 Security Level** is **AuthNoPriv** or **AuthPriv**
SNMPV3 Auth Password	The password for this authorization type.	Required if **Connectivity Type** is **SNMPv3** and **SnmpV3 Security Level** is **AuthNoPriv** or **AuthPriv**
SNMPV3 Priv Type	These SNMPv3 Privacy Types are supported: • CFB_AES_128 • CBC_DES_56 • AES-192 • AES-256 • 3-DES	Required if **Connectivity Type** is **SNMPv3** and **SnmpV3 Security Level** is **AuthPriv**
SNMPV3 Priv Password	The password for this privilege type.	Required if **Connectivity Type** is **SNMPv3** and **SnmpV3 Security Level** is **AuthPriv**

Edit credential profiles

To edit credential profiles, complete these steps.

Warning If you change the settings in a credential profile without first changing the settings on the associated device, you might lose connectivity, be unable to collect some KPI data, or be unable to execute configured playbooks on devices associated with the modified profile. For example, if the SNMP community string on the device does not match the value in the credential profile, SNMP-based KPIs will not function.

Before you begin

- Export a CSV backup of the profiles you want to change. Refer to Export credential profiles for instructions.
- Change settings on any associated devices.

Procedure

Step 1 Choose **Device Management** > **Credentials**.

Step 2 Select the profile check box for the profile you want to update. Click  .

Step 3 Make the necessary changes and then click **Save**.

Note
If the device is not updated within 30 seconds after you modify connectivity or credential profile information, move the device state to DOWN and then UP. This action triggers CLI reachability, and the updated values are displayed.

Export credential profiles

When you export credential profiles, the system saves the selected profiles in a CSV file. You can use this CSV file to quickly create backup copies of your credential profiles. You can edit the CSV file as needed and re-import it to add new credential profiles or modify existing data.

The exported credential profiles CSV file does not contain real passwords or community strings. All the characters in the password and community string entries are replaced with asterisks. If you plan to modify and re-import the CSV file, use asterisks instead of actual passwords or community strings. To replace the asterisks with actual values after importing, see Edit credential profiles, on page 244 for instructions.

Procedure

Step 1 Choose **Device Management** > **Credential Profiles**.

Step 2 (Optional) In the **Credential Profiles** page, filter the credential profile list as needed.

Step 3 Select the profile check boxes for the profiles you want to export.

Step 4 Click  . Depending on your browser, you will be prompted to select a path and file name for saving the CSV file, or to open the file immediately.

Delete credential profiles

To delete a credential profile, complete these steps:

Note You cannot delete a credential profile that is associated with one or more devices or providers.

Procedure

Step 1 Export a backup CSV file that contains the credential profile you plan to delete. For instructions, refer to Export credential profiles, on page 245.

Step 2 Check whether any devices or providers are using the credential profile you plan to delete. To do this, filter on the **Credential Profile** column. This column is available in the **Devices** window (choose **Device Management** > **Credential Profiles**) and in the Providers window (choose **Administration** > **Manage Provider Access**).

Step 3 Reassign the devices or providers to a different credential profile. For instructions, see Change the credential profile for multiple network devices, on page 246 and Edit provider settings, on page 289.

Step 4 After all devices and providers have had their credential profiles reassigned, from the main menu, choose **Device Management** > **Credential Profiles**.

Step 5 In the **Credential Profiles** window, choose the profile that you want to delete and then click  .

Change the credential profile for multiple network devices

If you want to change the credential profile for many network devices, it is often more efficient to edit device information in a CSV file. The process includes these steps:

1. Export a CSV file containing the devices whose credential profiles you want to change. Refer to Export device information to a CSV file, on page 317 for instructions.
2. Edit the CSV file, changing the credential profile for each device (this credential profile must already exist).
3. Save the edited file.

The credential profile linked to these devices must include the authorization credentials for each protocol configured during onboarding. If any protocol-specific credentials are missing or incorrect in the profile, the CSV import will succeed, but reachability checks for these devices will fail.

Before you begin

Ensure that the credential profile you intend to switch to already exists; otherwise, the CSV import will fail. If you haven't created the necessary credential profile, do so before proceeding.

Procedure

Step 1 From the main menu, choose **Device Management** > **Devices**. The **Network Devices** tab is displayed by default.

Step 2 Choose the devices whose credential profiles you want to change. Your options are:

- Click  to include all devices.
- Filter the device list by entering text in the **Search** field or by filtering specific columns. Then click  to include only the filtered list of devices.
- Check the boxes next to the device records you want to change. Then click  to include only the devices that have been checked.

Step 3 Edit and save the new CSV file using the tool of your choice. Be sure to enter the correct credential profile name in the **Credential Profile** field for each device.

Step 4 Click  .

Step 5 In the **Import** dialog box, click **Browse**, choose the new CSV file, and click **Import**.

Providers

Crosswork Network Controller components depend on external services, such as Cisco Crosswork Network Services Orchestrator (NSO) and Segment Routing Path Computation Element (SR-PCE), to perform operations like configuration modifications and segment routing path calculations. To manage access and facilitate information sharing among Crosswork Network Controller components, each external service must have a configured provider that belongs to a specific provider family (for example, NSO or SR-PCE).

A provider family is a service grouping that

- specifies the type of external service offered to the Crosswork Network Controller, and
- defines the parameters unique to the service type.

The system stores provider connectivity details and makes this information available to applications interacting with those external platforms.

For more information, refer to Providers in the *Before you begin* section of the **Get Up and Running (Post-Installation) chapter** of the guide.

Provider families

Crosswork Network Controller supports different types, or families, of providers. Each provider family supplies its own mix of special services, and each comes with unique requirements and options.

Table 32: Supported provider families

Provider family	Description
NSO	Instances of Cisco Network Services Orchestrator (Cisco NSO), used to configure network devices. See Add a Cisco NSO provider, on page 257.
SR-PCE	Instances of Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) containing the configuration information needed to allow Cisco Crosswork applications to communicate with and retrieve segment routing information for the network. See Add SR-PCE providers, on page 267.
WAE	Instances of Cisco WAN Automation Engine (Cisco WAE) provide "what if" analysis used to evaluate network changes. See Add Cisco WAE providers, on page 283 .

Provider family	Description
Syslog Storage	Instances of storage servers (remote or on the Cisco Crosswork application VM itself) where you want to store syslogs and other data retrieved from devices by KPIs and playbooks. See Add syslog storage providers, on page 284.
Alert	Instances of providers (such as Cisco Crosswork Situation Manager) to which alerts collected during KPI monitoring are to be forwarded. See Add an alert provider, on page 285
Proxy	Instances of proxy providers. See Add proxy providers, on page 286
Accedian (ACCEDIAN_PROXY)	Instances of Accedian Skylight providers. See Add Accedian Skylight as provider for more details.

Provider dependency

This section explains the provider configurations required for each system component.

Table 33: Provider dependency matrix

Cisco Crosswork Network Controller Component	Provider Type					
	NSO	SR-PCE	WAE	Syslog Storage	Alert	Proxy
Element Management Functions	Optional	Optional	Optional	Optional	Optional	Optional
Optimization Engine	Optional	Mandatory Required protocol is HTTP.	Optional	Optional	Optional	Optional
Active Topology	Mandatory Required protocols are HTTPS and SSH (for NSO backup)	Mandatory Required protocol is HTTP.	Optional	Optional	Optional	Optional
Service Health	Mandatory Required protocols are HTTPS and SSH (for NSO backup)	Mandatory Required protocol is HTTP.	Optional	Optional	Optional	Optional
Change Automation	Mandatory Required protocols are HTTPS and SSH (for NSO backup)	Optional	Optional	Optional	Optional	Optional

Cisco Crosswork Network Controller Component	Provider Type					
	NSO	SR-PCE	WAE	Syslog Storage	Alert	Proxy
Health Insights	Mandatory Required protocols are HTTPS and SSH (for NSO backup)	Optional	Optional	Optional	Optional	Optional

Note Configuring a syslog storage provider with Change Automation and an alert provider with Health Insights is beneficial but not mandatory.

Manage Provider Access

The **Manage Provider Access** page allows you to easily access tasks to create and manage providers. To navigate to this page, choose **Administration** > **Manage Provider Access**.

Figure 64: Manage provider access page

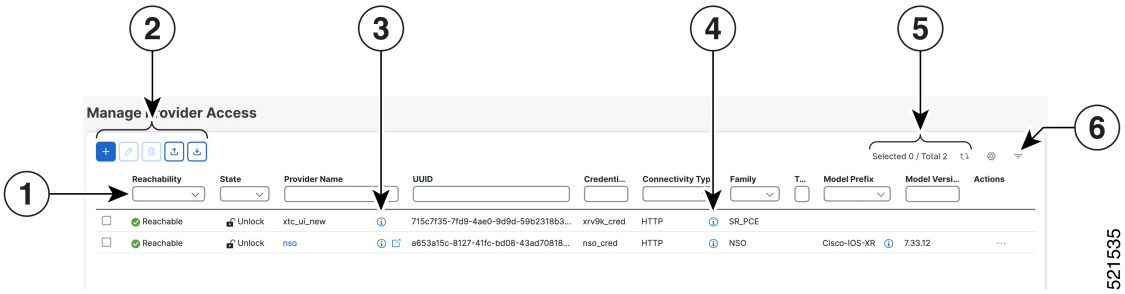


Table 34: Manage provider access page items

Item	Description
1	The icon shown next to the provider in this column indicates the provider's **Reachability**.

Item	Description
2	Click to add a provider. See Add a provider, on page 250.
	Click to edit the settings for the selected provider. See Edit provider settings, on page 289.
	Click to delete the selected provider. See Delete providers, on page 290.
	Click to import new providers or update existing providers from a CSV file. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file. See Import multiple providers using a CSV file, on page 253.
	Click to export a provider to a CSV file. See Export providers, on page 290.
3	Click next to the provider in the **Provider Name** column to open the **Properties** pop-up window, showing the details of any startup session key/value pairs for the provider.
4	Click next to the provider in the **Connectivity Type** column to open the **Connectivity Details** pop-up window, showing the protocol, IP, and other connection information for the provider.
5	Click to refresh the **Providers** window.
	Click to choose which columns are visible in the Providers window.
6	Click to set filter criteria on one or more columns in the **Providers** window.
	To clear a filter, click the corresponding [X] in the Filters menu.

Avoid topology sync issues during provider updates

Wait for the system to respond before making another provider update. For example, leave a pause between adding, deleting, or reading providers. If actions are performed too quickly, topology services may not reflect the changes. If you notice that topology is not synchronized, restart the topology service.

Add a provider

Before you begin

Review the configuration requirements for your provider family. For more information, see Provider families, on page 247.

Use this procedure to add a new external provider. Once you add the provider, you can map it to the managed devices.

To add a provider, complete these steps:

Procedure

Step 1 Choose **Administration** > **Manage Provider Access** > .

Step 2 Enter required provider details. For specific field definitions, see Add provider window fields, on page 251.

Step 3 Click **Save** to add the new provider.

Step 4 Repeat the steps to add more providers.

Add provider window fields

The table lists the Add Provider window fields and their descriptions.

Table 35: Fields in the Add Provider window (*=Required)

Field	Description
*** Provider Name**	The name for the provider that will be used to refer to it in the Cisco Crosswork application. For example: **`Linux_Server`**. The name can contain up to 128 alphanumeric characters, as well as dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.
*** Credential profile**	Select the name of the credential profile that is used by the Cisco Crosswork application to connect to the provider.
*** Family**	Select the provider family.
Connection type(s)	
*** Protocol**	Select the principal protocol to be used to connect to the provider. For information on provider configurations required for each system component, see Provider dependency, on page 248 matrix. To add more connectivity protocols for this provider, click at the end of the first row. To delete a protocol you have entered, click shown next to that row. You can enter multiple sets of connectivity details, including those for the same protocol.
*** Server details**	Select and provide one of these options: • IP Address (IPv4 or IPv6) and subnet mask of the provider's server. • FQDN (domain name and host name)
*** Port**	Enter the port number to use to connect to the provider's server. This is the port corresponding to the protocol being configured. For example, if the protocol used to communicate with the provider server is SSH, the port number is usually 22.
Timeout(sec)	Enter the amount of time (in seconds) to wait before the connection times out. The default is 30 seconds.

Field	Description
*** Encoding type**	Required if you are adding a Accedian_proxy provider. The available options are JSON, BYTES, PROTO, ASCII, and JSON IETF. Based on device capability, each device supports a single encoding format at a time.
Model prefix info **Note** The **Model** and **Version** fields do not apply to single VM deployments of Crosswork Network Controller.	
*** Model**	Required if you are adding a Cisco NSO provider: Select the model prefix that matches the NED CLI used by Cisco NSO. Valid values are: • `Cisco-IOS-XR` • `Cisco-NX-OS` • `Cisco-IOS-XE` For telemetry, only `Cisco-IOS-XR` is supported. To add more model prefix information for this Cisco NSO provider, click the ⊕ at the end of any row in the **Model Prefix Info** section. To delete a model prefix you have entered, click the ⊗ shown next to that row.
*** Version**	Required only if you are adding a Cisco NSO provider: Enter the Cisco NSO NED driver version used on the NSO server.
Provider properties	
Property key	Enter the name of the key for the special provider property you want to configure. Provider properties determine how the Cisco Crosswork Network Controller component interacts with each provider. The need for these properties and their types vary by provider family. Additional details are documented in topics dedicated to adding specific providers in this guide. The system does not validate provider properties. Ensure that you enter properties valid for the provider. **Note** In a two network interface configuration, the Cisco Crosswork applications default to communicating with providers using the Management Network Interface (`eth0`). You can change this behavior by adding **Property key** and **Property value** as `outgoing-internal` and `eth1` respectively. This is most often necessary when creating the SR-PCE provider, as its management interface may reside on the data network instead of the management network.
Property value	Enter the value to assign to the property key. To add more special properties for this provider, click ⊕ at the end of any key/value pair in the **Provider properties** section. To delete a key/value pair you have entered, click ⊗ shown next to that pair.

Import multiple providers using a CSV file

Before you begin

Importing providers from a CSV file adds any providers not already in the database, and overwrites any existing providers with the same name. For this reason, export a backup of all your current providers before starting the import. For instructions, see Export providers, on page 290.

Use this task to quickly onboard several providers at once. To create a CSV file that specifies providers and then import it into the Crosswork Network Controller, complete these steps:

Procedure

Step 1 Choose **Administration** > **Manage Provider Access**.

Step 2 Click to open the **Import providers** panel.

Step 3 If you have not already created a provider CSV file to import:

a) Click the **Download sample 'Provider template (*.csv)' file** link and save the CSV file template to a local storage resource.

b) Open the template using your preferred tool. Begin adding rows to the file, one row for each provider.

Use a semicolon to separate multiple entries in the same field. Use two semicolons (;;) with no space between them to indicate that you are leaving the field blank. When you separate entries with semicolons, the order in which you enter values is important. For example, if you enter **`SSH;SNMP;NETCONF;TELNET`** in the **connectivity_type** field and you enter **`22;161;830;23`** in the **connectivity_port** field, the order of entry determines the mapping between the two fields:

- SSH: port 22
- SNMP: port 161
- NETCONF: port 830
- Telnet: port 23

Delete any sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

c) Save the completed CSV file.

Step 4 Click **Browse**, select your completed CSV file and click **Open**.

Step 5 With the CSV file selected, click **Import**.

The provider information you imported should now be displayed in the **Providers** window.

Step 6 Review the import results. Resolve any errors reported during the import and verify provider details to confirm connection.

Cisco NSO providers

Network Services Orchestrator (NSO) acts as the configuration engine enabling service and transport provisioning, including VPN services and segment routing policies. Crosswork Network Controller integrates

NSO providers to offer unified device lifecycle management, service orchestration, and visualization, providing a single pane of glass for network and service views. Cisco NSO providers in Crosswork Network Controller serve as a network management component that:

- enables Crosswork Network Controller to configure devices based on their expected functions,
- allows optional configuration of MDT sensor paths for data collection, and
- delivers essential device management, configuration, and maintenance services.

NSO function packs

The Cisco NSO sample function packs offer a starting point for VPN service provisioning functionality in Crosswork Network Controller. While some samples can be used “as is” in limited network configurations, they are intended to demonstrate the extensible design of Crosswork Network Controller.

- For answers to common questions, consult Cisco DevNet or Cisco Customer Experience representatives.
- Support for further customization of samples for your specific use cases can be arranged through your Cisco account team.
- See View Installed NSO Function Packs to monitor the state of the installed NSO function packs.
- The NSO Function Pack deployment via Crosswork Network Controller UI is supported for NSO system installation and as a root user. For detailed deployment information, see the *Cisco Crosswork Network Controller 7.1 Installation Guide*.

Requirements for adding NSO providers

Required configurations for adding NSO providers

Ensure these configuration requirements are met prior to adding an SR-PCE provider.

- Create a credential profile for the Cisco NSO provider. For instructions, see Create credential profiles, on page 240.
- Confirm Cisco NSO device configurations. For more information, see Configuration sample for Cisco NSO devices, on page 305.

Required information for adding NSO providers

You must have this information when adding a SR-PCE provider.

- The name you want to assign to the Cisco NSO provider.
- The Cisco NSO NED device models and driver versions used in your topology. You can find the Cisco NSO version using the `version` command.
- The Cisco NSO server IP address or FQDN (Domain name and host name). When NSO is configured with HA, use the management VIP address as the IP address.
- The NSO cross launch feature is not available for user roles with read-only permissions.

NSO layered service architecture (LSA) deployment

Crosswork Network Controller supports the deployment of Cisco NSO Layered Service Architecture (LSA). An NSO layered service architecture is a network management framework that

- supports deployment of multiple device nodes for improved memory usage and provisioning throughput,
- organizes NSO providers into customer-facing (CFS) and resource-facing (RFS) roles for service management, and
- automates the identification and role assignment of each NSO provider to streamline operations and scalability.

In an LSA deployment, only one CFS provider is permitted. This provider encompasses all services, while RFS (resource-facing service) providers manage individual devices. On the **Manager Provider Access** page, the **Type** column identifies whether the NSO provider is CFS.

Key considerations for NSO LSA deployment

- Enable LSA settings before adding an NSO LSA provider. For details, see Enable layered service architecture (LSA), on page 255.
- If LSA settings are not enabled or provider property values are misconfigured, perform the recommended recovery steps mentioned in the NSO LSA setup recovery, on page 256 section.
- Ensure that RFS node IP addresses configured on the CFS match those shown in the user interface. A mismatch generates the error: "LSA cluster is missing RFS providers."
- For a CFS node, only the **`forward`** property key is used.

Enable layered service architecture (LSA)

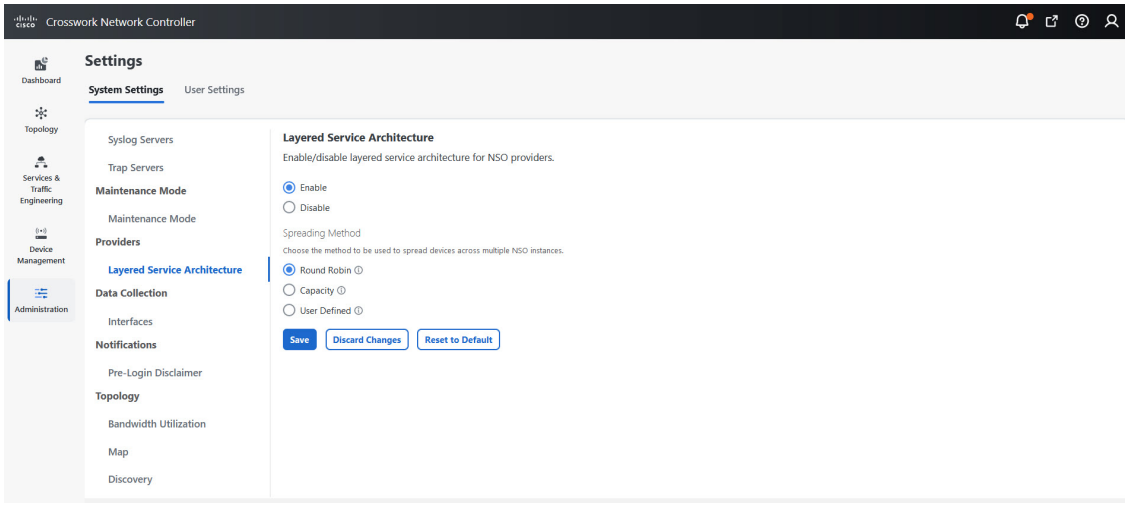
Use this procedure to configure LSA. This provides scalability by spreading network devices across multiple NSO instances, using your preferred distribution method.

To enable LSA, complete these steps.

Procedure

Step 1 Choose **Administration** > **Settings** > **System settings** > **Layered service architecture**.
The **Layered service architecture** page appears.

Figure 65: Layered service architecture page



Step 2 Select **Enable**.

Step 3 Select the method to distribute devices across multiple NSO instances:

- **Round Robin**: Evenly distributes devices to RFS nodes in a cyclical manner (for example, Device 1 to RFS1, Device 2 to RFS2, and so on).
- **Capacity**: Assigns devices to each RFS instance based on its available capacity.
- **User Defined**: Assigns devices to specific NSO providers as specified in the device settings. For more details, see Add devices individually through the UI, on page 309.

Step 4 Click **Save**.

Note
After saving, you cannot disable LSA without first removing all NSO providers.

NSO LSA setup recovery

Use this procedure to recover a misconfigured NSO LSA setup.

To recover the LSA setup, complete these steps.

Procedure

Step 1 Remove the NSO providers and associated devices in Device Management.

Step 2 Clean up the associated services in the Cisco NSO application.

Step 3 Enable LSA settings and add the the NSO LSA provider with correct property values.

Step 4 Add the NSO providers and devices again to Crosswork Network Controller, and map them to the Crosswork Data Gateway.

Step 5 Perform the sync operation on the NSO nodes (RFS and CFS) to sync the devices correctly.

The NSO LSA functionality is recovered as expected.

Embedded NSO for single VM deployment

Crosswork Network Controller deployed on a single VM with the Advantage package, uses an embedded NSO instead of an external NSO. The embedded NSO comes bundled as part of the Crosswork Network Controller Advantage package and is automatically installed when the package is deployed on a single VM.

When the embedded NSO is installed on the Crosswork Network Controller:

- An NSO provider entry is automatically onboarded on the Providers page.
- An SSO service provider entry supporting NSO cross-launch is automatically added on the SSO page.
- The embedded NSO provider and the SSO service provider entries cannot be edited or deleted.

Add a Cisco NSO provider

Before you begin

- Ensure all Requirements for adding NSO providers, on page 254 are met.
- Create a credential profile for NSO if one does not already exist.

Use this procedure to when you need to enable device onboarding and management between Cisco NSO and Crosswork Network Controller.

Attention Crosswork Network Controller does **not** continuously scan NSO for device status changes. New device addition to NSO is discovered only when there is an explicit action in Crosswork Network Controller that interacts with NSO.

To onboard newly added devices from NSO to Crosswork Network Controller, perform an NSO action or update and save the NSO provider policy details.

- Perform any NSO action for a device (from **Device Management** > **Network Devices**.
- Edit and save the policy details of an existing NSO provider (select **Actions > Edit policy details >** set **Onboard from** to **TRUE > Save**) to trigger Crosswork Network Controller to rescan NSO.

To add a Cisco NSO provider, complete these steps:

Procedure

Step 1 Choose **Administration** > **Manage Provider Access** >  .

Step 2 Enter these provider field values:

a) **Provider name**: Enter a name for the provider.

b) **Credential profile**: Select the previously created Cisco NSO credential profile.

c) **Family**: Select **NSO**.

d) Configure connection properties:

- **Protocol**: Select **HTTPS** and/or **SSH**. For more information, see Provider dependency, on page 248 matrix.

  Note
  To use the **Backup NSO** option during backup, configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail.

- **Server details**: Provide the IP address (IPv4 or IPv6) or FQDN (domain or host name) of the server.

  Important
  If you update the IP address or FQDN of the NSO provider, detach and reattach devices from the associated virtual data gateway. If you fail to do this, the provider changes will not be reflected in MDT collection jobs.

- **Server details**: Provide the IP address (IPv4 or IPv6) or FQDN (domain or host name) of the server.
- **Port**: Enter the appropriate port number. For HTTPS, enter the port that corresponds with what is configured on the NSO VM in etc/ncs/ncs.conf to access NSO using HTTPS. NSO uses **8888** as default port.
- **Timeout** (Optional): Enter the amount of time (in seconds) to wait before timing out the connection to the NSO server. The default is 30 seconds.

Note
If you set the **Site location** parameter in NSO, you can determine if geo-fencing is violated during testing when Crosswork Network Controller and the active NSO are not in the same site location. Crosswork Network Controller will also raise and clear alarms if a geo-fence violation is detected.

e) Configure the model prefix information:

- **Model**: Select Cisco-IOS-XR, Cisco-NX-OS, or Cisco-IOS-XE. Add a model for each type of device that will be used in the topology. If you have more than one, add another supported model.
- **Version**: Enter the NED software version installed for the device model in NSO.

f) For **Provider properties**, enter the key and value pairs as needed.

Property key	Value
forward	Set to **true** if you need to allow provisioning operations from the Crosswork Network Controller UI and enable the northbound interface to NSO through the Crosswork API gateway. **Note** The default value of **forward** is "false". If this is not changed, devices added to Crosswork Network Controller will not be added to NSO. This setting is used in conjuction with the **Edit Policy** option (see Edit the NSO provider policy, on page 260).

Property key	Value
nso_crosslaunch_url **Note** For NSO standalone providers only.	Enter the URL to enable cross-launching NSO application from the Crosswork Network Controller UI. Example format: **https://<NSO IP address/FQDN>: port number** Requires a valid protocol (**HTTP** or **HTTPS**), and the provider must be reachable. The cross launch icon ( ) is displayed in the **Provider Name** column. Alternately, you can cross launch the NSO application using the launch icon located at the top right corner of the window.
input_url_prefix **Note** For NSO LSA providers only.	Enter the RFS ID. Example format: **/rfc-x**, where **x** refers to the number of the RFS node. For RFS node 1: `input_url_prefix: /rfc-1`

Step 3 Click **Save**.

What to do next

(Optional) Configure the NSO site name, on page 259

Configure the NSO site name

You can configure the site name for NSO from the NCS backend. The site name appears as a read-only value on the NSO provider in the Crosswork Network Controller UI.

To configure the NSO site name, complete these steps.

Procedure

Step 1 Log in to ncs_cli in configuration mode.

Step 2 Set `hcc dns member master ip-address nso1-mgmt-IP location site1-location`

Step 3 Set `hcc dns member standby ip-address nso2-mgmt-IP location site2-location`

Step 4 Commit your changes.

View installed NSO function packs

Crosswork Network Controller allows you to monitor the operational status of installed NSO function packs.

To view installed NSO function packs, complete these steps.

Procedure

Step 1 Choose **Administration** > **Crosswork Manager**.

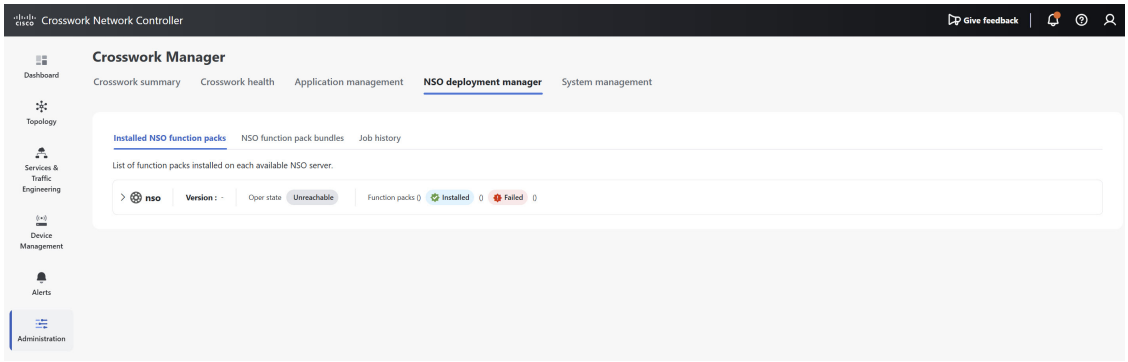
Step 2 On the **Crosswork Manager** window, select the **NSO deployment manager** tab.

The **Installed NSO function packs**, **NSO function pack bundles**, and **Job history** tabs are displayed.

Note
You can also access this view from NSO provider entries in the **Providers** page by choosing **Actions** > **View function packs**.

The **Installed NSO function packs** tab lists all NSO function pack bundles deployed on the NSO server.

Figure 66: Installed NSO function packs



Step 3 Expand the bundles to view the number of function packs within each bundle, the function pack name, operational state (**Up** or **Down**), description, and version number.

Edit the NSO provider policy

Edit the NSO provider policy when you need to modify how devices are matched, onboarded, synchronized, or managed between Crosswork Network Controller and NSO.

To edit an NSO provider policy, complete these steps.

Procedure

Step 1 Choose **Administration** > **Manage Provider Access**.

Step 2 On a NSO provider, click **Actions** > **Edit policy details**.

The **Edit policy details** page for the selected NSO provider is displayed.

Step 3 Update the policy configuration fields to meet the specific requirements of your environment, ensuring the values align with your discovered devices. You can modify each criteria to define a targeted subset of devices and fine-tune the actions that DLM will perform.

For example, when a device's configuration is changed, DLM will attempt to sync with NSO and apply all relevant rules, such as MatchRule, OnboardToNSO, OnboardToRule.

The different attributes you can edit within the NSO policy are:

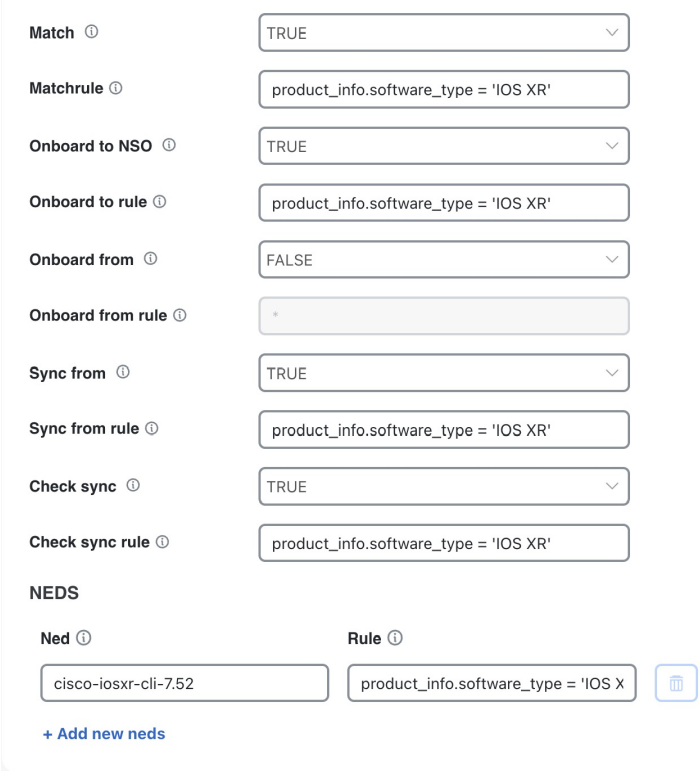
Table 36: Editable policy attributes

Attribute	Description
Match	Set to **True** to match Crosswork Network Controller devices with those in NSO based on their IP address.
MatchRule	Enter an expression defining the subset of devices.
Onboard To NSO	Set to **True** to add missing devices to NSO.
Onboard To Rule	Enter an expression for onboarding a subset of devices.
Onboard From	Set to **True** to onboard devices from NSO to Crosswork network Controler if they are missing.
Onboard From Rule	Enter an expression for onboarding devices from NSO.
Sync From	Set to **True** to sync-from the NSO device after onboarding.
Sync From Rule	Enter an expression defining the subset of devices for sync-from.
Check Sync	Set to **True** to check sync status of NSO devices.
Check Sync Rule	Enter an expression for the subset of devices for check-sync.
NED	Specify the Network Element Driver (NED) to be used. By default, the latest CLI NED on NSO is used.
Rule	Enter an expression to define which devices should use a specific NED.

Step 4 Review your changes and click **Save**. The NSO policy rules are applied every time DLM synchronizes with NSO.

Specifying a NED for IOS-XR devices

The following image shows the policy attributes that set the cisco-iosxr-cli-7.52 NED for IOS-XR devices with a software version 6.23.



The entry for defining **Rule** is partially visible. Here is the complete text for your reference:

product_info.softwaretype='IOS XR' and product_info.softwareversion='6.23'

You can specify different criteria such as hostname, software type, and IP address and use operators like Eq (=), Neq (!=), GT (>), LT (<), GTEQ (>=), LTEQ (<=) and EqA (= =) to define the comparisons. Here are few more examples of expressions you can use to edit provider details:

- **Device information**
  - host_name = 'host1'
  - product_info.manufacturer = 'Cisco Systems'
  - profile!='simulators'
- **Software and product details**
  - product_info.software_type = 'IOS XR'
  - product_info.softwareversion = '6.23'
  - product_info.producttype = 'Cisco IOS XRv 9000 Router'
  - product_info.productfamily = 'Routers'
  - product_info.productseries = 'Cisco ASR 9000 Series Aggregation Services Routers'
- **Routing information**
  - routing_info.router_loopback.inet_addr = '10.10.10.10'

- routing_info.te_router_id = '10.8.8.52'

- **Combining criteria**
  - Use the AND, OR commands to combine criteria. For example:

    product_info.software_type = 'IOS XR' OR product_info.software_type = 'IOS XE'

    product_info.software_type = 'IOS XR' AND product_info.software_version = '7.0.1'

- **Using wildcards**

  Use the * symbol as a wildcard. For example, to match any IOS device, you can use IOS*. If no wildcard expression is used, the system performs an exact match of the string.

  - **Exact match example**

    If product_info.software_type = 'IOS XR' is specified, DLM matches only the devices where the software_type is exactly 'IOS XR'.

  - **Wildcard example**

    If product_info.software_type = 'IOS XR*' is specified, DLM matches all devices where the software_type starts with 'IOS XR'. This includes values such as 'IOS XR 1', 'IOS XRv'.

Note For more information about editing NSO provider details and forming expressions using the attributes available in the Crosswork Inventory API, refer to the link DLM Inventory APIs.

Cisco SR-PCE providers

Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) providers

- supply device discovery, management, configuration maintenance, and route calculation services to Cisco Crosswork Network Controller components,
- enable system access as part of SDN controllers in the management domain, and
- support multi-AS topology and path calculations.

Requirements and additional information

Multi-AS topology and path calculations are supported if the complete topology is accessible to both the Crosswork Network Controller and each PCE. A single PCE cannot view a specific AS topology while another PCE views a different topology. Each PCE must have access to the entire topology view.

To learn and discover SR policies, Layer 3 links, and devices, at least one SR-PCE provider is required. Additionally, a second SR-PCE can be configured as a backup.

Requirements before adding SR-PCE providers

Required configurations for adding SR-PCE providers

Before adding an SR-PCE provider, ensure these configuration requirements are met to guarantee successful integration and operation.

- **Device and software requirements**: Configure a device to act as the SR-PCE. Enable SR for IS-IS or OSPF protocols according to your device platform documentation, and configure an SR-PCE. For example, refer to the *Segment Routing Configuration Guide for Cisco NCS 540 Series Routers*.

Note SR-PCE is only supported on the Cisco IOS XRv 9000 platform.

- **Credential profiles**: Create a credential profile for the Cisco SR-PCE provider (see Create credential profiles) with these connection types:
  - gRPC: Required to discover topology, SR-MPLS, and SRv6 policies. See Sample PCE configuration for enabling gRPC API on XR for configuration examples.
  - Basic HTTP text-authentication: Required to process for RSVP, TreeSID and PCEP sessions. MD5 authentication is currently not supported.

    If the Cisco SR-PCE server you are adding does not require authentication, you must still provide a credential profile for the provider. Select a profile that does not use the HTTP protocol.

- **gRPC with TLS (Optional)**: If setting up gRPC with Transport Layer Security (TLS), a certificate must be generated and added with the **Provider gRPC communication** role. The certificate secures TLS communication between gRPC clients and the EMS server. The client should use ems.pem and ca.cert to initiate the TLS authentication. To update the certificate, copy the newly generated certificate to the required location and restart the server. For more details, refer to the *Manage Certificates* chapter in this guide..
- **High availability**: For high availability, set up two separate Cisco SR-PCE providers with unique names and IP addresses, but with matching configurations.

Required information for adding SR-PCE providers

You must have this information when adding a SR-PCE provider:

- The name you want to assign to the Cisco SR-PCE provider. This is usually the DNS hostname of the Cisco SR-PCE server.
- The Cisco SR-PCE server IP address.
- The interface you want to use to communicate between Cisco SR-PCE and the Crosswork Network Controller server.
- SSH credentials for the PCE device to enable gRPC communication. PCE API credentials are used exclusively for HTTP-based communication.
- Determine whether to auto-onboard devices that Cisco SR-PCE discovers and, if so, whether their management status should be set to **`off`**, **`managed`** or **`unmanaged`** when added.

Requirements for auto-onboarding managed devices

If you plan to auto-onboard devices that the Cisco SR-PCE provider discovers and set them to a managed state in the database:

- Assign an existing credential profile for communication with the new managed devices.
- Configure the credential profile with an SNMP protocol.

TLS configurations for SR-PCE

A TLS configuration is a network security feature that:

- provides encrypted communication between SR-PCE and Crosswork applications
- leverages existing gNMI certificates for simplified certificate management
- supports server authentication (client authentication planned for future release), and
- ensures compliance with network security requirements.

TLS is enabled by default in SR-PCE gRPC configurations. Upload valid certificates and configure the trust chain in Crosswork to ensure secure communication.

How TLS works with gRPC API

When TLS is enabled:

1. SR-PCE presents its certificate to connecting clients
2. Clients validate the certificate against the configured root CA
3. An encrypted channel is established for all gRPC communications
4. All API data transmission occurs over this secure channel

Configure TLS for gRPC API

Enable secure, encrypted communications for gRPC API in SR-PCE deployments using TLS, to protect data in transit and ensure compliance.

Configuring TLS for the SR-PCE gRPC API secures all API interactions using encryption. This process is essential in environments where data confidentiality and integrity are required, especially when using Crosswork Network Controller for device management.

Before you begin

Before configuring TLS for the SR-PCE gRPC API, make sure all prerequisites are met.

- SR-PCE access and readiness
  - SR-PCE is installed and operational
  - Administrative access to the SR-PCE CLI and file system is available.
- Certificates and keys
  - A Root CA certificate is available (used for gNMI collection).
  - Private key and certificate files are generated for SR-PCE.

Note Crosswork Network Controller supports only server authentication and not mutual authentication (client certificate validation).

Use these steps to configure TLS on SR-PCE for gRPC API:

Procedure

Step 1 Verify TLS configuration on SR-PCE.

TLS is enabled by default when gRPC is configured. Check your current settings.

a) Access the SR-PCE CLI.
b) Check the gRPC configuration:

```
show running-config grpc
```

c) Ensure that the gRPC has these configurations:

- `no-tls` is not configured under gRPC.
- `tls-mutual` is not enabled under gRPC (it is disabled by default).

gRPC configuration shows TLS enabled without mutual authentication.

Step 2 Prepare the certificates.

Before uploading certificates to SR-PCE, ensure you have the private key, certificate, and root CA certificate.

Important
The certificates must include the `basicConstraints` extension with `CA:False`, ensuring it cannot be used as a certificate authority or improperly delegated in a chain of trust.

Step 3 Upload certificates to SR-PCE.

a) Transfer the private key and certificate to SR-PCE using SCP or SFTP.
b) Copy files to the required locations:

```
cp your-private-key.pem /misc/config/grpc/ems.key
cp your-certificate.pem /misc/config/grpc/ems.pem
```

c) Verify that the file has read permissions:

```
ls -la /misc/config/grpc/
```

d) Restart the emsd process to load the new certificates:

```
process restart emsd
```

The process restarts successfully without errors.

Step 4 Configure the root CA certificate in Crosswork Network Controller UI.

If not already configured for gNMI collection:

a) Log in to Crosswork Network Controller UI.
b) Navigate to **Administration** > **Certificate Management**.
c) Click the + icon to add a new certificate.

d) Configure the certificate:

- Device Certificate Name: Enter a name for the certificate.
- Certificate Role: Select **`Provider gRPC Communication`**.
- Secure gRPC CA certificate trustchain: Upload your root CA .pem file.

e) Click **Save**.

Note
If a gNMI certificate already exists and multiple trust chains are needed, update the existing .pem file to include all required CA certificates.

After successful addition, the gNMI Certificate appears in the Certificates listed in **Certificate Management > Certificates**.

The gRPC configuration displays TLS enabled without mutual authentication.

What to do next

After configuration, verify that TLS is functioning correctly.

1. Check the emsd process status:

```
show process emsd
```

2. Review gRPC service status:

```
show grpc status
```

3. Check logs for TLS-related errors:

```
show logging | include TLS
show logging | include grpc
```

4. Test connectivity from a gRPC client using TLS.

Related Topics

Certificates, on page 369
Add a new certificate, on page 377

Add SR-PCE providers

Before you begin

Ensure the configuration requirements defined in Requirements before adding SR-PCE providers, on page 263 are met prior to adding an SR-PCE provider.

To add one or more Cisco SR-PCE providers, complete these steps:

Procedure

Step 1 Choose **Administration** > **Manage Provider Access** >  .

Step 2 Enter these SR-PCE provider field values:

a) **Provider**: Enter a name for the SR-PCE provider.
b) **Credential profile**: Select the credential profile you created for the SR-PCE provider.
c) **Family**: Select **SR_PCE**.
d) Configure connection properties.

- **Connection type(s) > Protocol**:
  - Select **HTTP** and enter required fields. HTTP is required to process RSVP, TreeSID and PCEP sessions. The default port is 8080.
  - Select **GRPC** or **GRPC_SECURE** (gRPC with Transport Layer Security (TLS)) and enter required fields. These settings are required to process topology, SR-MPLS, and SRv6 policies. Only one of these options can be used. If GRPC_SECURE is selected, you must provide the trusted certificate in the **Certificate profile** field.
- **Server details**: Enter the server IP address (IPv4 or IPv6) and subnet mask.
- **Port**: Enter the port number.
- **Timeout** (Optional): Enter the amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

e) **Provider properties**: Enter property keys and values:

Table 37: Property keys

When the property key is..	And the value is..	Then..
auto-onboard	off	when devices are discovered, the device data is recorded in the Cisco SR-PCE database, but is not registered in the Crosswork Network Controller Inventory Management database. **Note** Use this option if you plan to manually (via UI or CSV import) enter all of your network devices.
	unmanaged	all devices that Crosswork Network Controller discovers will be registered in the Crosswork Network Controller Inventory Management database, with their configured state set to **unmanaged**. SNMP polling will be disabled for these devices, and no management IP information will be included. To get these devices into the **managed** state later, you will need to either edit them via the UI or export them to a CSV, make modifications and then import the updated CSV. You can also assign credential profiles by adding them to the device CSV file before import (the credential profiles must already exist).
	managed	all devices that Cisco SR-PCE discovers will be registered in the Crosswork Network Controller Inventory Management database with their configured state set to **managed**. Typically suitable for an environment that has same device profiles, devices are managed by their TE router-ID, and all devices can be discovered by the Cisco SR-PCE. SNMP polling will be enabled for these devices, and Cisco SR-PCE will also report the management IP address (TE Router ID for IPv4, or IPv6 Router ID for IPv6 deployment). The devices will be added with the credential profile associated with the device-profile key in the SR-PCE provider configuration. Important considerations If you enable this option for IPv6 deployment, devices will still register as **unmanaged** in the inventory. When you delete an onboarded device that was added via SR-PCE discovery with auto-onboard set to **managed**, the topology service adds it again as **unmanaged**. This ensures that devices that have been removed are not automatically managed again unless they acquire a new TE-ID. To manage a rediscovered device, update its status manually.
device-profile	a credential profile name	if the **auto-onboard** is set to **managed** and there is no valid **device-profile** set, the device will instead be onboarded as **unmanaged**.

When the property key is..	And the value is..	Then..
outgoing-interface	eth1	this enables Crosswork Network Controller access to SR-PCE via the data network interface when using a two NIC configuration.
preferred-stack	ipv4	indicates a dual stack is present and IPv4 is preferred.
	ipv6	indicates dual stack is present and IPv6 is preferred.
	NOT SET	indicates no dual stack.
pce	off	discovery of RSVP-TE tunnels and PCEP sessions (required for all LSP provisioning) is disabled.
	on	discovery of RSVP-TE tunnels and PCEP sessions (required for all LSP provisioning) is enabled. This option is enabled by default.
topology	any value	there is no impact. This property key is deprecated and should be manually removed if it still appears as an option. This property key is ignored, regardless if it is configured.

Important considerations when using property keys:

- Topology can be visualized even with **auto-onboard** as **off** and a **device-profile** is not specified.
- If **managed** or **unmanaged** options are set and you want to delete a device later, you must either:
  - Reconfigure and remove the devices from the network before deleting the device from Crosswork Network Controller. This avoids Crosswork Network Controller from rediscovering and adding the device back.
  - Set **auto-onboard** to **off**, and then delete the device from Crosswork Network Controller. However, doing so will not allow Crosswork Network Controller to detect or auto-onboard any new devices in the network.
- If you want to upgrade a device, change its state to **unmanaged** before starting the upgrade. After completing the upgrade, return the device to the **UP** state.
- It is not recommended to modify **auto-onboard** options once set. If you need to modify them:
  1. Delete the provider and wait until deletion confirmation is displayed in the **Events** window.
  2. Add the provider again with the updated **auto-onboard** option.
  3. Confirm the provider has been added with the correct **auto-onboard** option in the **Events** window.

Step 3 Click **Save** to add the SR-PCE provider.

Step 4 Confirm that the SR-PCE provider shows a green Reachability status without any errors. You can also view the Events window to see if the provider has been configured correctly.

Step 5 Repeat this process for each SR-PCE provider.

What to do next

- If **auto-onboard** is set to **off**, start onboarding devices.
- If you opted to automatically onboard devices, choose **Device Management** > **Network Devices** to view the device list. To add more node information such as geographical location details, export the device list (.csv), update it, and import it back. If geographical location data is missing, you will only be able to see device topology using the logical map.

Cisco SR-PCE reachability issues

Use this procedure to resolve Cisco SR-PCE connectivity problems and restoring real-time topology status updates and notifications.

You can find SR-PCE reachability issues raised in the Events table and reachability status in the **Providers** page. Refer to Get provider details, on page 288 for details. If the SR-PCE goes down, the system displays all topology links in their last known state, and you stop receiving topology updates and notifications. When SR-PCE connectivity resumes, the Events table ( ) shows a reconnection message and the topology is updated accordingly.

You can troubleshoot reachability in these ways:

Procedure

Step 1 Check device credentials.

Step 2 Ping the provider host to verify network connectivity.

Step 3 Attempt a connection using the protocols specified in the provider's connectivity settings. For an SR-PCE provider, it is typically HTTP and port 8080.

Step 4 Check firewall rules and network configurations to ensure they are not blocking required ports or services.

Step 5 Check for Access Control List (ACL) settings on the Cisco SR-PCE host or any intervening devices that might restrict access.

Step 6 If the SR-PCE remains unreachable for a long period, or the system is not syncing or updating, delete the SR-PCE and add it again when connectivity returns.

a) Execute the following command on the SR-PCE host to restart the process:

```
# process restart pce_server
```

b) Choose **Administration** > **Manage Provider Access** and delete the SR-PCE provider. On restoring connectivity, add the provider again.

Multiple Cisco SR-PCE HA pairs

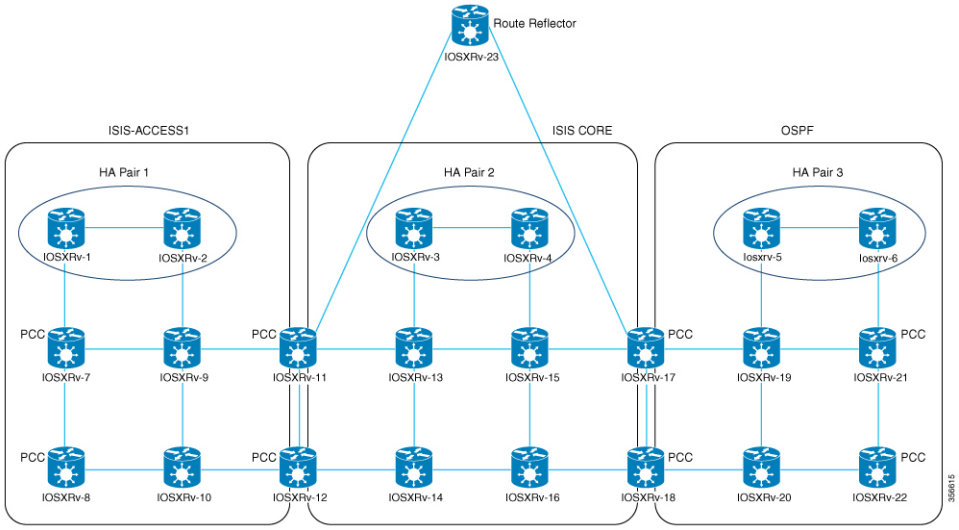
Multiple Cisco SR-PCE HA pairs allow network operators to deploy up to eight redundant SR-PCE pairs for greater overall system resilience and scalability. Each HA pair of Cisco SR-PCE providers must have matching configurations and must support the same network topology. If one SR-PCE in a pair becomes unreachable, the system uses the secondary SR-PCE to discover the network topology. If both fail, the next HA pair takes over and so forth. The network topology will continue to be updated correctly and you can view SR-PCE connectivity events in the Events table ( ).

Multiple HA pair behavior

In the case of multiple SR-PCE HA pairs, each SR-PCE pair sees the same topology and manages only the tunnels created from its Path Computation Clients (PCCs). The figure shows a sample of a three SR-PCE HA pair topology.

- HA Pair 1—PCE iosxrv-1 and iosxrv-2 *only* provision and discover tunnels whose headends are iosxrv-7 and iosxrv-8. Note that iosxrv-9 and iosxrv-10 are not PCC routers.
- HA Pair 2—PCE iosxrv-3 and iosxrv-4 *only* provision and discover tunnels whose headends are iosxrv-11, iosxrv-12, iosxrv-17, and iosxrv-18. Note that iosxrv-13, iosxrv-14, iosxrv-15, and iosxrv-16 are not PCC routers.
- HA Pair 3—PCE iosxrv-5 and iosxrv-6 *only* provision and discover tunnels whose headends are iosxrv-21 and iosxrv-22. Note that iosxrv-19 and iosxrv-20 are not PCC routers.

Figure 67: Sample 3 HA pair topology



Note When multiple SR-PCE HA pairs are configured, the SR-PCE used for topology discovery is selected randomly based on which SR-PCE responds first. All SR-PCEs across all HA pairs must maintain the same complete network topology to ensure consistent network operations.

Configure HA

The following configurations must be done to enable each pair of HA Cisco SR-PCE providers to be added in Crosswork Network Controller.

Note There must be resilient IPv4 connectivity between both SR-PCEs to enable HA. The PCE IP address of the other SR-PCE should be reachable by the peer at all times.

Issue this commands on *each* Cisco SR-PCE device:

Enable the interface:

```
# interface <interface><slot>/<port>
ipv4 address <sync-link-interface-ip-address> <subnet-mask>
no shut
```

Enable HA:

```
# pce api sibling ipv4 <other-node-pce-address>
```

Establish a sync link between the two SR-PCEs:

```
# router static
address-family ipv4 unicast
<other-node-pce-ip-address>/<subnet-mask-length> <remote-sync-link-ip-address>
```

(Optional) `# pce segment-routing traffic-eng peer ipv4 <other-node-pce-ip-address>`

It should be entered for each PCC and not for other PCE nodes.

Enter this command on the PCC:

For SR Policies: `# segment-routing traffic-eng pcc redundancy pcc-centric`

For RSVP-TE Tunnels: `# mpls traffic-eng pce stateful-client redundancy pcc-centric`

Confirm sibling SR-PCE configuration

From the SR-PCE, enter the `show tcp brief` command to verify that synchronization between SR-PCEs in HA are intact:

```
#show tcp brief | include <remote-SR-PCE-router-id>
```

Confirm the information is correct:

Local address	Foreign address	State
<local-SR-PCE-router-id>:8080	*<remote-SR-PCE-router-id>*:*<any-port-id>*	ESTAB
<local-SR-PCE-router-id>:*<any-port-id>*	*<remote-SR-PCE-router-id>*:8080	ESTAB

For example:

```
RP/0/0/CPU0:iosxrv-1#sh tcp brief | i 192.168.0.2:
Mon Jun 22 18:43:09.044 UTC
0x153af340 0x60000000 0 0 192.168.0.1:47230 192.168.0.2:8080 ESTAB
0x153aaa6c 0x60000000 0 0 192.168.0.1:8080 192.168.0.2:16765 ESTAB
```

In this example, 192.168.0.2 is the remote SR-PCE IP.

SR-PCE delegation

Depending on where an SR-TE policy is created, the following SR-PCE delegation occurs:

- SR-PCE initiated—Policies configured on a PCE. SR-TE policies are delegated back to the source SR-PCE.

Note

- The policy can be PCE initiated even if it is created using the UI, but in that case it is not configured explicitly on SR-PCE.
- RSVP-TE tunnels cannot be configured directly on a PCE.

- PCC initiated—An SR-TE policy or RSVP-TE tunnel that is configured directly on a device. The SR-PCE configured with the lowest precedence is the delegated SR-PCE. If precedence is not set, then SR-PCE with the lowest PCE IP address is the delegated SR-PCE. The configuration example, shows that **10.0.0.1** is assigned a precedence value of 10 and will be the delegated SR-PCE.

```
segment-routing
  traffic-eng
    pcc
      source-address ipv4 10.0.0.2
      pce address ipv4 10.0.0.1
        precedence 10
       !
      pce address ipv4 10.0.0.8
        precedence 20
       !
       report-all
       redundancy pcc-centric
```

For RSVP-TE Tunnel:

```
mpls traffic-eng
interface GigabitEthernet0/0/0/0
!
interface GigabitEthernet0/0/0/1
!
interface GigabitEthernet0/0/0/2
!
pce
  peer source ipv4 192.168.0.02
  peer ipv4 192.168.0.9
    precedence 10
  !
  peer ipv4 192.168.0.10
    precedence 20
  !
  stateful-client
   instantiation
   report
   redundancy pcc-centric
   autoroute-announce
  !
!
auto-tunnel pcc
  tunnel-id min 1000 max 5000
```

- Crosswork Network Controller SR-PCE initiated—An SR-TE policy that is configured using Crosswork Network Controller. SR-PCE delegation is random per policy.

Note Only SR-TE policies or RSVP-TE tunnels created by Crosswork Network Controller can be modified or deleted by Crosswork Network Controller.

HA notes and limitations

- It is assumed that all PCCs are PCEP connected to both SR-PCEs.
- When an SR-PCE is disconnected only from Cisco Crosswork, the following occurs:
  - SR-PCE delegation assignments remain, but the SR-PCE that has been disconnected will not appear in Crosswork Network Controller.
  - You are not able to modify Cisco Crosswork SR-PCE initiated SR-TE policies if the disconnected SR-PCE is the delegated PCE.
- In some cases, when an SR-TE policy that was created via the UI is automatically deleted (intentional and expected) from Crosswork Network Controller, a warning message does not appear. For example, if the source PCC is reloaded, the UI created SR policy disappears and the user is not informed.
- In an extreme case where one SR-PCE fails on all links (to PCCs/topology devices) except the up-link to Crosswork Network Controller, topology information will not be accurate in Crosswork Network Controller. To resolve this, fix the connectivity issue or delete both SR-PCEs from the Provider page and re-add the reachable one.
- **PCE HA failover:** After a PCE HA failover, when Crosswork Network Controller connects to the next available PCE, the Topology Service could take up to **2 hours** to re-learn all L3 links and LSPs depending on the scale. During this time, newly created LSPs will remain in the queue and only appear in the UI after re-learning is complete.
- When an SR-PCE goes down, **Local Congestion Mitigation** (LCM) enters a dormant stage. To exit this state, all SR-PCEs must be connected, and their associated topologies fully synchronized with the topology service. LCM will remain dormant until these conditions are met. It is important to note that LCM does not have visibility into the state of the SR-PCE redundancy set.

SR-PCE configuration examples

The following configurations are *examples* to guide you in a multiple SR-PCE setup for HA. Please modify accordingly.

ISIS single topology configuration for dual-stack networks

Cisco Crosswork Network Controller supports ISIS Single Topology in addition to Multi-Topology. To utilize this, your XTC devices must be configured for ISIS Single Topology. For Single Topology configurations, only global IPv6 addressing is supported; support for link-local IPv6 addressing is not included.

Device-side configuration example

```
RP/0/RP0/CPU0:iosxrv-2(config)#router isis [NAME]
RP/0/RP0/CPU0:iosxrv-2(config-isis)#address-family ipv6 unicast
RP/0/RP0/CPU0:iosxrv-2(config-isis-af)#single-topology
```

Configuration requirements for deploying and reporting SR MSL policies to PCE

Enable gRPC on devices and for SR-TE policies

```
RP/0/RP0/CPU0:L1-NCS5501#sh running-config grpc
grpc
 segment-routing
  traffic-eng
   policy-service
  !
```

```
 !
 port 57400
 no-tls
```

Advertise all SR policies to BGP-LS peers

This configuration enables your router to report all configured SR MSL policies—both active and inactive—into the link-state database. As a result, these policies can be advertised via BGP-LS to controllers or peers, providing full visibility and supporting network orchestration.

```
RP/0/RP0/CPU0:L1-NCS5501#sh running-config segment-routing traffic-eng distribute link-state

segment-routing
 traffic-eng
  distribute link-state
   report-candidate-path-inactive
  !
 !
!
```

Prevent reporting MSL policies in PCEP

This configuration prevents SR MSL policies from being reported via PCEP. Since PCEP does not fully support MSL policies (it only advertises a single segment list, which can cause operational issues), it is recommended to remove the report-all command from the PCC configuration on the headend router.

```
RP/0/RP0/CPU0:L4-NCS560#sh running-config segment-routing traffic-eng pcc
segment-routing
 traffic-eng
  pcc
   source-address ipv4 192.100.0.4
   pce address ipv4 100.100.0.1
    precedence 25
   !
   pce address ipv4 100.100.0.2
    precedence 50
   !
   !  Remove the following line to prevent reporting MSL policies to PCE
   !  report-all
   redundancy pcc-centric
   profile 1981
    autoroute
     include ipv4 all
     force-sr-include
    !
   !
  !
 !
!
```

Advertise SR MSL policies in link-state to PCE neighbor via BGP-LS

This configuration enables your router to advertise SR MSL policies in the link-state address family to a PCE neighbor over BGP. By establishing a BGP session with the PCE and including the `address-family link-state link-state` configuration, the router ensures that SR MSL policies are advertised and can be learned by the PCE.

Note The link-state address family must be configured on both the headend and the PCE for successful exchange.

```
RP/0/RP0/CPU0:L1-NCS5501#sh running-config router bgp
router bgp 60
```

```
 neighbor <NEIGHBOR_IP>   ! PCE neighbor
  remote-as 60
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
  address-family ipv6 unicast
  !
  address-family link-state link-state. ! Enable BGP-LS for SR MSL policy advertisement
  !
 !
```

SRv6 data collection and traffic steering for DDM (Deterministic Demand Matrix) integration on Cisco IOS XR

Enable SRv6 locator accounting

This configuration enables the router to perform detailed accounting for IPv6 traffic specifically related to SRv6 locators. By tracking traffic on a per-prefix and per-nexthop basis, operators gain granular visibility into the usage and flow of SRv6-enabled services.

```
RP/0/RP0/CPU0:L1-NCS5501#sh running-config accounting
accounting
 prefixes
  ipv6
   mode per-prefix per-nexthop srv6-locators
  !
 !
!
```

Enable SRv6 accounting data to telemetry

This configuration sets up model-driven telemetry on the router to stream SRv6 accounting data to external collectors. By defining specific sensor paths, the router can push operational data related to SRv6 locator accounting, enabling real-time monitoring, analysis, and orchestration of SRv6 network performance and traffic patterns.

```
RP/0/RP0/CPU0:L1-NCS5501#sh running-config telemetry model-driven
telemetry model-driven
 sensor-group cisco_models
  sensor-path
Cisco-IOS-XR-infra-xtc-agent-oper:xtc/forwarding/policy-forwardings/policy-forwarding
  sensor-path
Cisco-IOS-XR-fib-common-oper:cef-accounting/vrfs/vrf[vrf-name='default']/afis/afi[afi-type=ipv6]/pfx/srv6locs/srv6loc

 !
!
```

Enable customer/VRF traffic steering to SRv6 locators via BGP

This configuration enables an edge router to steer customer or VRF (Virtual Routing and Forwarding) IPv4 and IPv6 traffic into specific SRv6 locators using BGP.

```
RP/0/RP0/CPU0:L1-NCS5501#sh running-config router bgp
router bgp 60
 bgp router-id <ROUTER_ID_IP>
 segment-routing srv6
  locator L1algo0
 !
 address-family ipv4 unicast
  network <ROUTER_ID_IP>/32
 !
 address-family vpnv4 unicast
  vrf all               ! If there are multiple VRF where traffic is ingressing, add srv6
```

```
 locator in vrf all.
   segment-routing srv6
    locator L1algo0
    alloc mode per-vrf
   !
  !
 !
 vrf ntt
  rd 200:200
  address-family ipv4 unicast
   segment-routing srv6   ! If there is only one VRF where traffic is ingressing, add srv6
 locator in this vrf alone, if there is no VRF, then add the locator in neighbor address
family
    locator L1algo0
    alloc mode per-vrf
   !
   redistribute connected
  !
  neighbor <NEIGHBOR_IP>
   remote-as 61
   update-source GigabitEthernet0/0/0/0
   address-family ipv4 unicast
    route-policy PASS_ALL in
    route-policy PASS_ALL out
   !
  !
 !
```

Verify SRv6 traffic steering via CEF accounting

This command is used to verify that IPv6 traffic is being steered into SRv6 locators, rather than MPLS labels, by inspecting the CEF accounting statistics. It provides granular visibility, showing packet and byte counts for specific IPv6 prefixes that are associated with SRv6 locators.

```
sh cef ipv6 accounting
fccc:cc3e:3::/48
Accounting: 0/0 packets/bytes output (per-prefix-per-path mode)
 via fe80::2/128, Bundle-Ether1201
  path-idx 0
  next hop fe80::2/128
  Accounting: 200000/58400000 packets/bytes output  <<< Traffic packets for prefix
fccc:cc3e:3::
```

Other sample SR-PCE configurations

Redundant SR-PCE configuration (on PCE with Cisco IOS-XR 7.x.x)

```
pce
 address ipv4 100.100.0.7
 state-sync ipv4 100.100.0.1
 api
  sibling ipv4 100.100.0.1
```

PCE configuration for enabling gRPC API on XR 25.2.1.x (IPv4 deployment)

```
conf t
  lslib-server
  !
  grpc
    port 57400
    no-tls
    address-family ipv4
    service-layer
```

```
    !
!
pce
  distribute link-state
  !
!
linux networking
  vrf default
    address-family ipv4
      default-route software-forwarding
    !
    address-family ipv6
      default-route software-forwarding
    !
  !
!
commit
```

Note For secure gRPC deployment, remove `no-tls`.

Configure distribute link-state on all PCEs to inject SR policies into BGP-LS.

Enable gRPC API on XR 25.2.1.x (IPv6 deployment)

```
conf t
  lslib-server
  !
  grpc
    port 57400
    no-tls
    address-family ipv6
    service-layer
    !
!
pce
  distribute link-state
  !
!
linux networking
  vrf default
    address-family ipv4
      default-route software-forwarding
    !
    address-family ipv6
      default-route software-forwarding
    !
  !
!
commit
```

Note For secure gRPC deployment, remove `no-tls`.

Configure distribute link-state on all PCEs to inject SR policies into BGP-LS.

Verify whether the topology is published in gRPC

```
sh lslib server topology-db
```

Verify the SR-MPLS LSP published in gRPC

```
show lslib server topology-db detail protocol sr
```

Redundant SR-PCE configuration (PCC)

```
segment-routing
 traffic-eng
  pcc
   source-address ipv4 100.0.0.1
   pce address ipv4 100.0.0.2
    precedence 200
   !
   pce address ipv4 100.0.0.3
    precedence 100
   !
   report-all
   redundancy pcc-centric
```

Redundant SR-PCE configuration (on PCC) for RSVP-TE

Note `Loopback0` represents the TE router ID.

```
ipv4 unnumbered mpls traffic-eng Loopback0
!
mpls traffic-eng
 pce
  peer source ipv4 200.100.200.1
  peer ipv4 209.165.0.6
   precedence 200
  !
  peer ipv4 100.100.0.0
   precedence 100
  !
  stateful-client
   instantiation
   report
   redundancy pcc-centric
   autoroute-announce
  !
 !
 auto-tunnel pcc
  tunnel-id min 1000 max 1999
 !
!
```

Sample Telemetry configuations

SR-TM configuation

```
telemetry model-driven
 destination-group crosswork
  address-family ipv4 5.5.5.5 port 9000
   encoding self-describing-gpb
   protocol tcp
  !
 !
 sensor-group SRTM
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels
  sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes
```

```
 !
 subscription OE
  sensor-group-id SRTM sample-interval 60000
  destination-id crosswork
  source-interface Loopback0
!
traffic-collector
 interface GigabitEthernet0/0/0/3
 !
 statistics
  history-size 10
```

Note The destination address uses the southbound data interface (eth1) address of the Crosswork Data Gateway VM.

It is required to push sensor path on telemetry configuration via NSO to get prefix and tunnel counters. It is assumed that the Traffic Collector has been configured with all the traffic ingress interface. This configuration is needed for demands in the Bandwidth on Demand feature pack to work.

Telemetry sensor path

```
sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes/prefix
```

Telemetry configuration pushed by Crosswork Network Controller to all the headend routers via NSO

```
telemetry model-driven
  destination-group CW_43dc8a5ea99529715899b4f5218408a785e40fce
    vrf default
    address-family ipv4 5.5.5.5 port 30500
      encoding self-describing-gpb
      protocol top
    !
  !
destination-group CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  vrf default
  address-family ipv4 5.5.5.5 port 30500
    encoding self-describing-gpb
    protocol top
  !
!
sensor-group CW_43dc8a5ea99529715899b4f5218408a785e40fce
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
!
sensor-group CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  sensor-path
Cisco-IOS-XR-infra-tc-oper:traffic-collector/vrf-table/default-vrf/afs/af/counters/prefixes/prefix
!
subscription CW_43dc8a5ea99529715899b4f5218408a785e40fce
  sensor-group-id CW_43dc8a5ea99529715899b4f5218408a785e40fce sample-interval 300000
  destination-id CW_43dc8a5ea99529715899b4f5218408a785e40fce
!
subscription CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  sensor-group-id CW_4b3c69a200668b%a8dc155caff295645c684a8f8 sample-interval 300000
  destination-id CW_463c69a200668b0a8dc155caff295645c684a8f8
  !
!
```

Traffic Collector configurations

Traffic Collector configurations (all Ingress traffic interface to be added below in the Traffic Collector)

```
RP/0/RSP0/CPU0:PE1-ASR9k#sh running-config traffic-collector
Fri May 22 01:14:35.845 PDT
traffic-collector
  interface GigabitEthernet0/0/0/0
  !
  statistics
    history-size 1
    collection-interval 1
    history-timeout 1
    history-minute-timeout
  !
!
```

Add BGP neighbor next-hop-self for all the prefix (to show TM rate counters)

```
bgp router-id 5.5.5.5
address-family ipv4 unicast
  network 5.5.5.5/32
  redistribute static
!
address-family link-state link-state
!
neighbor 1.1.1.1
  remote-as 65000
  update-source Loopback0
  address-family ipv4 unicast
   next-hop-self
  !
!
```

Traffic collector tunnel and prefix counters

```
RP/0/RSP0/CPU0:PE1-ASR9k#show traffic-collector ipv4 counters prefix
Fri May 22 01:13:51.458 PDT
Prefix              Label         Base rate         TM rate        State
                                  (Bytes/sec)       (Bytes/sec)
------------------  ------------  ---------------  -------------  -----------------
1.1.1.1/32          650001         3                0              Active
2.2.2.2/32          650002         3                0              Active
3.3.3.3/32          650003         6                0              Active
4.4.4.4/32          650004         1                0              Active
6.6.6.6/32          650200         6326338          6326234        Active
7.7.7.7/32          650007         62763285         62764006       Active
8.8.8.8/32          650008         31129168         31130488       Active
9.9.9.9/32          650009         1                0              Active
10.10.10.10/32      650010         1                0              Active
RP/0/RSP0/CPU0:PE1-ASR9k#stt
RP/0/RSP0/CPU0:PE1-ASR9k#show traffic-collector ipv4 counters tunnel
Fri May 22 01:13:52.169 PDT
RP/0/RSP0/CPU0:PE1-ASR9k#]
```

Path computation client (PCC) support

A path computation client (PCC) is a network device that

- initiates path computation requests to an external path computation element (PCE),
- reports the status and attributes of label-switched paths (LSPs) such as RSVP-TE tunnels or SR policies, and

- establishes and manages Path Computation Element Protocol (PCEP) sessions with one or more PCEs for dynamic tunnel delegation and control.

Path computation clients (PCCs) can support delegation and reporting of multiple tunnel types, such as RSVP-TE tunnels and SR policies. For both functionalities to be supported on the same PCC, it is necessary to establish two separate PCEP connections with the PCEs. Each of these PCEP connections must use a unique source IP address, typically assigned to a loopback interface on the PCC.

Configuration example to set up PCEP connections for RSVP-TE tunnels on a Cisco IOS-XR

- The IP address 192.168.0.2 is the source IP for the PCEP session. This IP is assigned to a loopback interface on the router, ensuring stability and uniqueness.
- Two SR-PCEs are configured as peers for PCEP sessions. Each has a precedence value, with the lower precedence (10) indicating the preferred PCE for delegating RSVP-TE tunnels.
- An auto-tunnel PCC feature is configured with a range of tunnel IDs (from 10 to 1000). These IDs are assigned to RSVP-TE tunnels initiated by the PCE, such as those created by Cisco Crosswork Optimization Engine.

```
mpls traffic-eng
interface GigabitEthernet0/0/0/2
admin-weight 1
!
interface GigabitEthernet0/0/0/3
admin-weight 1
  pce
    peer source ipv4 192.168.0.2
    peer ipv4 192.168.0.1
      precedence 10
     !
    peer ipv4 192.168.0.8
      precedence 11
     !
    stateful-client
      instantiation
      report
     !
   !
   auto-tunnel pcc
    tunnel-id min 10 max 1000
   !
!
ipv4 unnumbered mpls traffic-eng Loopback0

rsvp
interface GigabitEthernet0/0/0/2
bandwidth 1000000
!
interface GigabitEthernet0/0/0/3
bandwidth 1000000
!
!
```

Add Cisco WAE providers

Before you begin

- Create a credential profile for the Cisco WAE provider. For instructions, see Create credential profiles, on page 240. This should be a basic HTTP/HTTPS text-authentication credential. MD5 authentication is

not supported. If the Cisco WAE server you are adding does not require authentication, you must still supply a credential profile, but it can be any profile that does not use the HTTP/HTTPS protocol.

- Know the name you want to assign to the provider. This is usually the DNS hostname of the Cisco WAE server.
- Know the Cisco WAE server IP address and port. The connection protocol will be HTTP or HTTPS.

Cisco WAN Automation Engine (Cisco WAE) providers supply traffic and topology analysis to the Crosswork Network Controller components. The foundation software is Cisco WAE Planning, which provides a cross-sectional view of traffic, topology, and equipment state. It takes advantage of a predictive model that performs "what if" analysis of failure impacts.

To add one or more Cisco WAE providers using the Crosswork Network Controller UI, complete these steps. To add providers by importing CSV files, refer to the instructions in Import multiple providers using a CSV file, on page 253.

Procedure

Step 1 Choose **Administration** > **Manage Provider Access** >  .

Step 2 Enter these provider field values:

a) **Provider name**: Enter a name for the Cisco WAE provider.
b) **Credential profile**: Select the credential profile you created.
c) **Family**: Select **`WAE`**.
d) Configure connection type properties:

- **Protocol**: Select **`HTTP`** or **`HTTPS`** as per the credential profile you are using.
- **Server details**: Enter the server IP address (IPv4 or IPv6) and subnet mask.
- **Port**: Enter the appropriate port number (usually **`8080`** for HTTP, and **`8843`** for HTTPS).
- **Timeout** (Optional): Enter the amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

Step 3 Click **Save** to add the provider.

Add syslog storage providers

Before you begin

- Create a credential profile for the storage provider. For instructions, see Create credential profiles, on page 240. This should be an SSH credential.
- Know the name you want to assign to the storage provider. This is usually the DNS hostname of the server.
- Know the storage provider's server IPv4 address and port. The connection protocol will be SSH.

- Know the destination directory on the storage provider's server. You will need to specify this using the **Provider properties** fields.

To add one or more storage providers using the Crosswork Network Controller UI, complete these steps. To add providers by importing CSV files, refer to the instructions in Import multiple providers using a CSV file, on page 253.

Procedure

Step 1 Choose **Administration** > **Manage Provider Access** >  .

Step 2 Enter these provider field values:

a) **Provider name**: Enter a name for the storage provider.

b) **Credential profile**: Select the credential profile you created.

c) **Family**: Select **`SYSLOG_STORAGE`**.

d) Configure connection type properties:

- **Protocol**: Select **`SSH`** as the protocol to connect the provider.
- **Server details**: Enter the server IP address (IPv4 or IPv6) and subnet mask.
- **Port**: Enter the appropriate port number (usually **`22`** for SSH).
- **Timeout** (Optional): Enter the amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

e) To configure provider properties, enter this key/value pair:

Property key: **`DestinationDirectory`**

Property value: The absolute path where the collected data will be stored on the server. For example: **`/root/cw-syslogs`**

Step 3 Click **Save** to add the provider.

Add an alert provider

Before you begin

- Create a credential profile for the alert provider. For instructions, see Create credential profiles, on page 240. This should be a basic HTTP text-authentication credential. MD5 authentication is not supported. If the provider does not require authentication, you must still supply a credential profile. It can be any profile that does not use the HTTP protocol.
- Know the name you want to assign to the alert provider. This is usually the DNS hostname of the server.
- Know the alert provider's server IPv4 address and port. The connection protocol will be HTTP.
- Know the URL of the alert server endpoint. You will need to specify this using the **Provider properties** fields.

An Alert provider is a destination to which you want to forward alerts collected during KPI monitoring (such as Cisco Crosswork Situation Manager). An alert provider must be capable of receiving and processing incoming alert packages. Currently, only one alert provider is supported.

To add an alert provider using the Crosswork Network Controller UI, complete these steps. To add an alert provider by importing CSV files, refer to the instructions in Import multiple providers using a CSV file, on page 253.

Procedure

Step 1 Choose **Administration** > **Manage Provider Access** >  .

Step 2 Enter these provider field values:

a) **Provider name**: Enter a name for the alert provider.

b) **Credential profile**: Select the credential profile you created.

c) **Family**: Select **`ALERT`**.

d) Configure connection type properties:

- **Protocol**: **`HTTP`** is pre-selected as the protocol to connect the provider.
- **Server details**: Enter the server IP address (IPv4 or IPv6) and subnet mask.
- **Port**: Enter the port number (usually **`80`** for HTTP).
- **Timeout** (Optional): Enter the amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

e) For provider properties, the **`alertEndpointUrl`** **Property key** is pre-entered. In the **Property value** field, enter the alert server endpoint only. For example, if the complete path to the endpoint is **`http://aws.amazon.com:80/myendpoint/bar1/`**, you would enter **`/myendpoint/bar1/`** only.

Step 3 Click **Save** to add the provider.

Add proxy providers

Before you begin

- Create a credential profile for each proxy provider. For instructions, see Create credential profiles, on page 240. This should be a basic HTTP or HTTPS text-authentication credential.
- Know the Resource Facing Service (RFS) node name added to the Customer Facing Service (CFS) node in your LSA cluster.
- Know the name you want to assign to the provider. This is usually the DNS hostname of the proxy server.
- Know the proxy server IP address and port. The connection protocol will be HTTP or HTTPS.
- Ensure the Cisco NSO providers have been added. For more information, see Add a Cisco NSO provider, on page 257.
- For NSO proxy provider, create a credential profile with **HTTP/HTTPS** with **Basic Authentication**.

- For ONC 1.0 proxy provider, create a credential profile with **HTTPS** with **Basic Authentication**.

You add a proxy providers to enable service provisioning through the Crosswork Network Controller interface. Crosswork Network Controller supports adding Cisco NSO and Cisco Optical Network Controller (ONC) v1.0 proxy providers.

- NSO APIs are directly accessible if NSO is configured with an external IP address.
- If NSO is deployed within a private network, then it will be reachable only through the Crosswork Network Controller interface. Proxy providers enables you to use Crosswork interface to perform service provisioning with NSO.

To add proxy providers, complete these steps:

Procedure

Step 1 Choose **Administration** > **Manage Provider Access** >  .

Step 2 Enter these provider field values:

a) **Provider name**: Enter a name for the proxy provider.

b) **Credential profile**: Select the credential profile you created.

Note
For ONC provider, select the profile configured with ONC TAPI APIs, not the ONC UI credentials.

c) **Family**: Select **`PROXY`**.

d) Configure connection type properties:

- **Protocol**: Select **`HTTP`** or **`HTTPS`**.
- **Server details**: Enter the IP address (IPv4 or IPv6) and subnet mask of the NSO cluster or the ONC 1.0 cluster VIP.
- **Port**: Enter the appropriate port number (usually **`30603`** for HTTPS).
- **Timeout** (Optional): Enter the amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

e) Configure **Provider properties** with these key and value pairs:

Table 38: For NSO proxy provider

Property key	Property value
`forward`	**`true`**
`input_url_prefix` **Note** Required only in case of RFS nodes.	**`/<rfs-node-name>`** <*rfs-node-name*> refers to the name of the RFS node added to the CFS node in the LSA cluster.

Table 39: For ONC 1.0 proxy provider

Property key	Property value
`forward`	`true`
`input_url_prefix`	`/onc-tapi`
`output_url_prefix`	`/crosswork/onc-tapi`

Step 3 Click **Save** to add the provider.

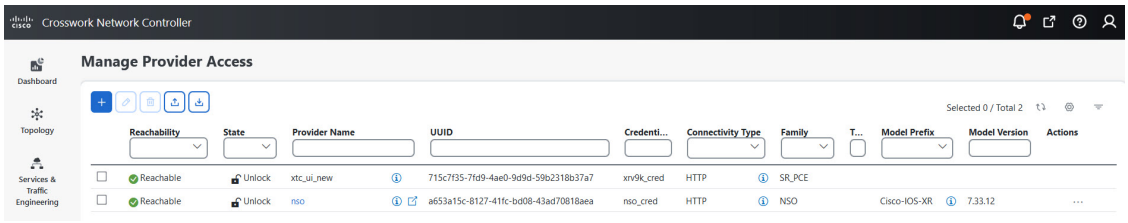
Get provider details

You can view details for each configured provider and check provider reachability in your Cisco Crosswork application. Use the **Providers** page to access information about each provider, including name, universally unique identifier (UUID), credential profile, and connectivity status. You can also view reachability status via different protocols.

Procedure

Step 1 Choose **Administration** > **Manage Provider Access**.
The **Providers** page displays all configured providers with details such as name, UUID, credential profile, and more.

Figure 68: Manage providers access



Step 2 The icons in the **Reachability** column indicate whether a provider is reachable via the listed connectivity protocols.

Provider reachability is checked automatically after you add or modify a provider. For Change Automation and Health Insights, ongoing checks occur approximately every 5 minutes. For SR-PCE via the Optimization Engine, checks occur every 10 seconds.

Note
Change Automation events and **Health Insights** events apply only to cluster deployments of the Crosswork Network Controller. **Optimization Engine** events applies in all cases except single VM deployments of the Crosswork Network Controller Essentials tier.

Step 3 To view additional details for a provider:

a) In the **Provider Name** column, click ⓘ to view provider-specific key/value properties.

b) In the **Connectivity Type** column, click ⓘ to view detailed connectivity information for the provider. This information includes protocol, IP format, IP address, port, and timeout values.

c) In the **Model Prefix** column, click to view the supported NED version(s) for a Cisco NSO provider's configured NED model prefix(es).

d) Click to exit the details window.

If you encounter SR-PCE reachability problems, ensure HTTP and port 8080 are set, and see Cisco SR-PCE reachability issues, on page 271.

For general provider reachability issues:

a. Ping the provider host.

b. Attempt a connection using the protocols specified in the provider's connectivity settings.

Use this CLI command to perform this check:

```
curl -v -H "X-Subscribe: stream" "http://<ip-address>:8080/
bwod/subscribe/json?keepalive-30&priority=5"
```

c. Check your firewall setting and network configuration.

d. Review Access Control List (ACL) settings on the provider host or intermediate devices that could restrict connectivity.

Edit provider settings

Before you begin

Export a CSV backup of the providers you want to change.

Use this procedure to update the settings for an existing provider. Provider changes can affect many devices in your network, potentially thousands in large environments.

Note

- Before editing any provider settings, make sure you understand the impact of your changes. If you are unsure about the potential risk of making a change, contact Cisco services for guidance.
- If modifying an SR-PCE provider, see related guidance in Add SR-PCE providers, on page 267 section; additional steps may be necessary.

To update an existing provider, complete these steps:

Procedure

Step 1 Choose **Administration** > **Manage Provider Access**.

Step 2 In the **Providers** window, select the provider to update and click .

Step 3 Make necessary changes and click **Save**.

Step 4 Resolve errors and confirm provider reachability.

The provider settings are updated and propagated to mapped devices.

Delete providers

Use this procedure to remove providers that are no longer needed. Delete providers only when they are not actively associated with devices or credential profiles. The system alerts you if associations exist.

To delete providers, complete these steps:

Procedure

Step 1 Export a backup CSV file containing the provider you plan to delete. For instructions, see Export providers, on page 290.

Step 2 (Optional) Check whether any devices are mapped to the provider and change the provider before deletion.

a) Choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed by default.
b) In the **Network Devices** window, enter the obsolete provider name in the **Search** field.
c) Select the device that is mapped to the obsolete provider, and click  .
d) Choose a different provider from the **Provider** drop-down list.
e) Click **Save**.

Step 3 Choose **Administration** > **Manage Provider Access**.

Step 4 In the **Providers** window, select the provider(s) to delete.

Step 5 Click  and confirm when prompted.

The selected providers are deleted if they are not associated with any devices or credential profiles.

Export providers

You can export provider data to a CSV file. This is a handy way to keep backup copies of your provider information.

Note You cannot edit a CSV file and then re-import it to update existing providers.

Procedure

Step 1 Choose **Administration** > **Manage Provider Access**.

Step 2 (Optional) In the **Manage Provider Access** page, filter the provider list as needed.

Step 3 Select the check boxes for the providers you want to export. To select all the providers for export, use the check box at the top of the column.

Step 4 Click  . Depending on your browser, you will be prompted to select a path and file name for saving the CSV file, or to open the file immediately.

The selected providers are exported to a CSV file.

Manage tags

A tag is a text identifier that you can attach to objects in the system. It helps

- group and categorize those objects, and
- enables users to identify, locate, and organize devices for varied purposes.

Crosswork Network Controller comes with a predefined set of tags (such as cli, mdt, reach-check, snmp, and clock-drift-check), which are automatically assigned to every device that is managed. These default tags cannot be selected, edited, deleted, or manually associated with any device.

You can create custom tags to group devices by type, geographic location, their network role (for example, spine vs. leaf), or function (Provider vs. Provider Edge)

Tag management page

Tags can provide information such as the device's physical location and its administrator's email ID, and are used to group devices. Use the **Tag Management** page to easily create and manage them.

To navigate to this page, choose **Administration** > **Tag Management**.

Figure 69: Tag management page

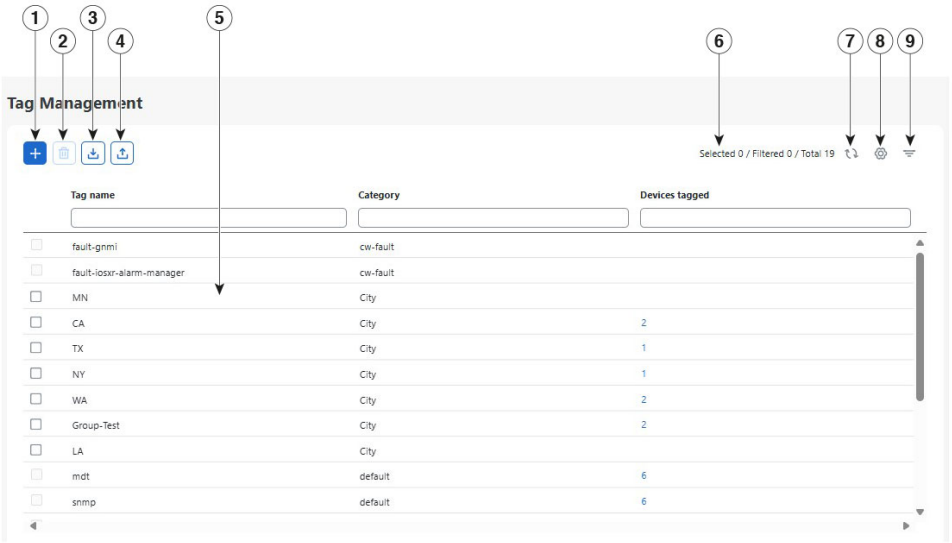


Table 40: Tag management page items

Item	Description
1	Click + to create new device tags. For instructions, see Create tags, on page 292.
2	Click 🗑 to delete currently selected device tags. For instructions, see Delete tags, on page 294.

Item	Description
3	Click to import the device tags defined in a CSV file into the Cisco Crosswork application. For instructions, see Import multiple tags using a CSV file, on page 293. You can also download a CSV file template by clicking this icon. The template includes sample data that you can use as a guide for building your own CSV file.
4	Click to export a CSV file that lists the tags that are currently configured and their attributes. You can update this file and import it back into the Cisco Crosswork application to quickly add or edit multiple tags. For instructions, see Export tags, on page 295.
5	Displays the tags and their attributes currently available in the Cisco Crosswork application.
6	Indicates the number of tags that are currently selected in the table.
7	Click to refresh the **Tag Management** page.
8	Click to choose the columns to make visible in the **Tag Management** page.
9	Click to set filter criteria on one or more columns in the **Tag Management** page.
	To clear a filter, click the corresponding [X] in the Filters menu.

Create tags

Creating tags makes it easier to organize, search, and filter managed objects. You can create up to 100 tags.

You can use a CSV file to efficiently import multiple tags. For instructions on importing multiple tags, see Import multiple tags using a CSV file.

Note Tag and tag category names are case-insensitive. They can contain up to 128 alphanumeric characters, as well as dots (.), underscores ("_"), or hyphens ("-"). No other special characters are allowed.

To create a tag, complete these steps:

Procedure

Step 1 Choose **Administration** > **Tag management** > . This displays the **Add tags** pane.

Step 2 Choose the tag category from the **Select tag category** drop-down list or type a new category's name in the text field and click **Add**.

Step 3 In the **Add tags for <category name>**, type a name for the new tag and press Enter.

Step 4 Click **Save**.

Note

If you enter a duplicate tag, the **Save** button remains disabled.

Import multiple tags using a CSV file

You can create a CSV file that lists the tags you want to apply to your devices, and then import it into the Cisco Crosswork applications. Importing multiple tags using a CSV file lets you efficiently create and update many tags and tag categories. This feature is valuable when you need to rapidly apply organizational tags to devices or make global tagging changes. The system automatically adds all new tags and tag categories from the CSV file to the database. It overwrites any existing tags with the same name. Consider exporting a backup of your current tags before starting the import.

Before you begin

Export a backup copy of your current tags. See Export tags, on page 295.

CSV file requirements

Your CSV file must include these fields:

Field	Description	Required or Optional
Tag Name	The name of the tag. For example: **`SanFrancisco`** or **`Spine/Leaf`**.	Required
Tag Category	The tag category. For example: **`City`** or **`Network Role`**.	Required

Note **Tag Name** and **Tag Category** fields are case-insensitive and can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are permitted.

To import multiple tags using a CSV file, complete these steps:

Procedure

Step 1 From the main menu, choose **Administration** > **Tag Management** > .

Step 2 If you have not already created a CSV file:

a) Click the **Download sample 'Tags template (*.csv)' file** link and save the CSV file template to a local device.

b) Open the template in your preferred editor. Add a row for each tag, using a comma to separate fields and a semicolon for multiple entries in the same field.

c) Check that your file meets the formatting rules above.

Tip
Be sure to delete the sample data rows before saving the file, or they will be imported along with the data you want. The column header row can stay, as it is ignored during import.

d) Save the new CSV file.

Step 3 Click **Browse** and select your completed CSV file.

Step 4 Click **Import** to upload it.

The tags and tag categories appear in the **Tag Management** page.

What to do next

Assign imported tags to devices. See Apply or remove device tags, on page 294 for instructions.

Apply or remove device tags

Tags and their categories are your main tool for grouping devices. Once you have tagged a set of devices with the same tag, they are considered part of a group, and you can manage them more easily. You can apply a maximum of 15 tags to any one device.

In order to apply a tag to a device or group of devices, the tag must already exist. See Create tags for more information.

For efficiency, Cisco Crosswork automatically updates inventory data, including topology, for all the devices in a tagged group, as a single set of inventory collection jobs. But please note that tag-group membership is static for other functions. For example, if you add or remove a device from a tagged group after applying a KPI, the KPI will monitor only the original group members. If you change group membership and want the KPI to monitor all the members of the group, re-apply the KPI to the changed group.

To apply tags to a device or set of devices, complete these steps:

Procedure

Step 1 Choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed, showing the list of devices.

Step 2 (Optional) If the list is long, click to set one or more filters and narrow the list to only those devices you want to tag.

Step 3 Check the check box next to the device(s) you want to tag. If you select multiple devices, any changes you make will be applied to all the devices you selected.

Step 4 Click . The **Edit tags** window opens, showing the tags currently applied to the device(s) you selected.

Step 5 Click in the **Associate tag** field and type the name of the tag you want to apply.

Step 6 Click on tag in the search result list to associate it with the device. To delete an applied tag, click the X icon shown next to that tag.

Step 7 Click **Save**.

Delete tags

Tags are used to group devices. Deleting them can affect which KPIs are monitored and which Playbooks are run when using Change Automation. Carefully review tag associations before deleting any tags.

To delete tags, complete these steps:

Note If the tag is mapped to any devices, then the tag cannot be deleted.

Procedure

Step 1 Export a backup CSV file containing the tags you plan to delete. See Export tags, on page 295 for instructions.

Step 2 Choose **Administration** > **Tag Management**. The **Tag Management** page is displayed.

Step 3 Select the check box next to the tags you want to delete and click .

Step 4 Review the confirmation dialog box. It lists the number of devices currently using the tag(s).

Step 5 Click **Delete** to confirm deletion.

The selected tags are deleted if not mapped to devices.

Export tags

You can export tags and tag categories to a CSV file for backup and editing. This allows you to create backup copies or edit tags offline, then re-import to overwrite existing tags. Note that after re-importing, you may need to re-associate devices and tags.

Procedure

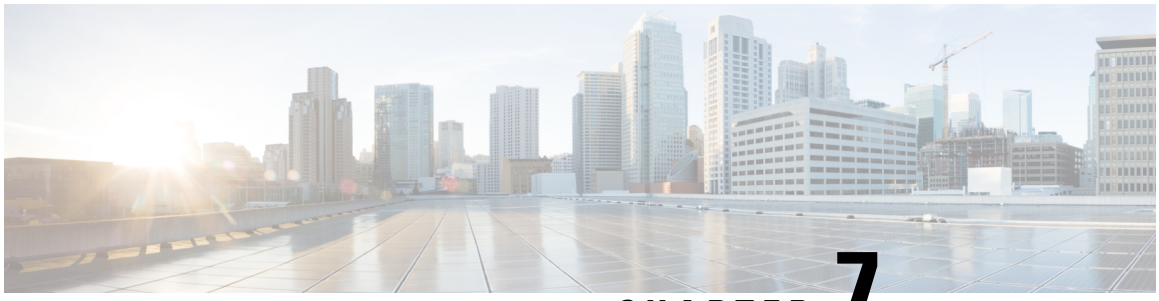
Step 1 Choose **Administration** > **Tag Management**.

Step 2 (Optional) In the **Tag Management** page, filter the tag list as needed.

Step 3 Select the check boxes for the tags you want to export. To select all tags, use the check box at the top of the column.

Step 4 Click . Depending on your browser, you will be prompted to select a path and file name for saving the CSV file, or to open the file immediately.

The selected tags and tag categories are exported to a CSV file.



CHAPTER 7

Add and Configure Devices

This section contains the following topics:

Device onboarding methods

A device addition is an onboarding mechanism that

- enables registration of network devices into Cisco Crosswork Network Controller,
- offers multiple supported methods tailored for different workflows, and
- requires specific prerequisites for each method to ensure successful onboarding.

Cisco Crosswork Network Controller supports dual-stack deployment. Devices can be onboarded with both IPv4 and IPv6 addresses. To prevent duplicate entries, onboard each device only once using either the IPv4 or IPv6 address.

There are different ways to add devices to Crosswork Network Controller:

1. Importing devices using the Crosswork APIs is the fastest and most efficient method, but it requires programming skills and API knowledge.

   For more information, see the CNC 7.2 API documentation.

2. Importing devices from a Devices CSV file is time-consuming. To use this method, you must first:
   - Create corresponding credential profiles for all of the devices and providers listed in the CSV file.

     For more information, see Manage credential profiles, on page 239.
   - Create the provider(s) that will be associated with the devices.

     For more information, see Providers, on page 247.
   - Create tags for use in grouping the new devices.

For more information, see Import multiple tags using a CSV file, on page 293.

- Download the CSV template file from Crosswork Network Controller and populate it with the devices you plan to add.

For information about adding devices using a CSV file, see CSV device imports, on page 315.

3. Adding devices via the UI is the least error-prone method because all data is validated during entry. However, this approach is time-consuming and is best for adding only a small number of devices at a time. Make sure device and provider credential profiles, as well as tags to be applied to them, are created before onboarding. For more information, see Add devices individually through the UI, on page 309.
4. Auto-onboarding from a Cisco SR-PCE provider is a highly automated and relatively simple method. Create device and provider credential profiles and any required tags before applying them to these devices. The auto-onboarding method does not create or assign device information automatically. Devices are initially discovered and added with partial information. To complete the onboarding process, you must supplement the missing details. You can provide the additional information by uploading a CSV file or manually adding it using the API or UI.

   For more information, see the provider properties in Provider families, on page 247.
5. Auto-onboarding using Zero Touch Provisioning is an automated process. First, create device entries and modify your installation's DHCP server. Make sure provider credential profiles and tags are created before use. After onboarding and provisioning, edit each device to supply any information not automatically added.

   For more information, see the *Zero Touch Provisioning*chapter in the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management Guide*.

Note If a device onboarded in Crosswork Network Controller shares a subnet with a Crosswork Data Gateway interface, ensure the device is on the data gateway's southbound network. Reverse Path Forwarding (RPF) checks in Crosswork Data Gateway require source addresses to be on the southbound network. Devices cannot use management or northbound networks if multiple NICs (2 or 3 NIC) are deployed.

Recommendations for efficient configuration

Prioritize consistent and secure device configuration

While configuring your devices for onboarding, review these guidelines:

- Use a common configuration file for all devices to enable reachability checks and consistent event collection.
- Plan for link discovery as part of the onboarding workflow. This approach requires necessary configuration work upfront, rather than addressing it incrementally. This is especially important to leverage configuration templates. Onboard devices without all the desired configurations initially and later push a standardized configuration to the devices. This ensures they are fully compatible with Crosswork Network Controller.
- Create unique SNMP EngineIDs for each device in the network.
- If a device's SNMP EngineID is reconfigured, recreate SNMP user accounts for that device.

- Limit NETCONF API access to users with privilege level 15. On XE devices where privilege level 15 is granted via **Enable Password**, do not use NETCONF for reachability or state verification.

Protect network access and validate device support

- If you are using TELNET in your network environments, implement security measures, such as firewall protections and ACLs to reduce any potential risks.
- If a device is onboarded with an unknown Sys Object ID, contact Cisco Customer Experience as the hardware may not be certified.

Configuration prerequisites for new devices

A configuration prerequisite is a set of device requirements that

- ensures a new device can be onboarded and managed by Crosswork Network Controller,
- covers key protocols and platforms, and
- prepares a device for streamlined integration into monitoring, telemetry, and orchestration workflows.

Devices need to be properly configured before onboarding to ensure compatibility with Crosswork Network Controller. Configuration details may vary by platform and use case, particularly for protocols such as SNMP, NETCONF, SSH, gNMI, syslog, and TELNET.

For specific protocols like LLDP, CDP, and LAG, see *Set Up and Use Your Topology Map* in the *Cisco Crosswork Network Controller 7.2 Administration Guide*.

Tip Planning for link discovery in advance helps complete required configuration upfront and simplifies later management, especially when leveraging configuration templates. You can onboard devices initially with partial configuration, using templates to standardize and complete the configuration later. This approach makes ongoing management and compliance with Crosswork requirements more efficient.

Requirements before onboarding devices

- Configure devices for pre-onboarding, on page 299
- Configure devices to forward events to Crosswork Network Controller, on page 300
- Configuration samples for new devices, on page 301

Configure devices for pre-onboarding

Prepare devices with standard protocol settings and rate limits before onboarding into Crosswork Network Controller.

Procedure

Step 1 Set logging for console and monitoring.

Step 2 Configure TELNET server limits.

Step 3 Configure SNMP communities and NTP.

Step 4 Generate SSH keys and configure session limits.

Step 5 Set NETCONF and XML agents, if MDT is supported.

The following commands provide a sample pre-onboarding device configuration that sets the correct SNMPv2 and NETCONF configuration, and SSH and TELNET rate limits.

```
logging console debugging
logging monitor debugging
telnet vrf default ipv4 server max-servers 100
telnet vrf default ipv6 server max-servers 100
crypto key generate rsa
 exec-timeout 0 0
 width 107
 length 37
 absolute-timeout 0
!
snmp-server community public RO
snmp-server community robot-demo2 RO
snmp-server ifindex persist
ntp
 server NTPServerIPAddress
!
ssh server v2
ssh server vrf default
ssh server netconf vrf default
ssh server logging
ssh server rate-limit 100
ssh server session-limit 100
!
netconf-yang agent
 ssh
!
netconf agent tty
!
xml agent tty
!
```

Configure devices to forward events to Crosswork Network Controller

Enable Crosswork Network Controller to receive SNMP traps and syslogs from managed devices for alarm and event management.

For most devices, this means you must configure the devices to forward SNMP traps and syslogs to the Data Gateway using its virtual IP as the receiver IP. If you have a geo high availability deployment, configure devices to forward events to both Data Gateway on the primary and secondary data center.

We recommend using a common configuration file for all your devices to allow Crosswork Network Controller to perform a reachability check and collect trap information.

Note When you configure a Data Gateway pool with spare Data Gateway, failover is handled without changing the IP address that devices use for forwarding traffic:

- If a Data Gateway fails, the spare Data Gateway automatically inherits the IP address of the failed Data Gateway.
- If your configuration uses an FQDN, traffic continues to route without disruption even if a Data Gateway in the pool fails because the FQDN remains unchanged.

Before you begin

- Confirm the Data Gateway pool virtual IP (*cdg_virtualIP*) addresses.
- In high-availability deployments, gather both primary and secondary Data Gateway addresses.

Configure a device to forward events to the Crosswork Network Controller server using the snmp-server host command:

Procedure

Step 1 Configure the device to send SNMP traps to the Data Gateway virtual IP.

Example:

```
snmp-server host 192.168.90.135 traps version 2c public udp-port 1062
```

Step 2 Set the SNMP community strings.

Example:

```
snmp-server community public RO
```

Step 3 Enable SNMP trap notifications for link status.

Example:

```
snmp-server traps snmp linkup
      snmp-server traps snmp linkdown
```

Step 4 Set the SNMP view group.

Example:

```
snmp-server view { group name } include
```

Step 5 In geo high-availability scenarios:

a) Add both primary and secondary Data Gateway addresses for redundancy.
b) If using FQDN, ensure the FQDN points to the Data Gateway pool.

Configuration samples for new devices

Before onboarding devices into Crosswork Network Controller, you must ensure that each device is configured according to the requirements of your platform and protocols.

These sections provide configuration examples for supported protocols and major operating systems. Use these reference samples as starting points and adapt the variable values to match your network environment. Review your platform documentation for version-specific requirements and verify that all configurations meet your organization's security and operational policies.

Configuration sample for Cisco IOS XR devices

These commands provide a sample pre-onboarding device configuration for IOS-XR devices.

Note that <SystemOwner> is a user-supplied variable.

```
snmp-server community community_name SystemOwner
snmp-server community community_name RO
snmp-server entityindex persist
snmp-server ifindex persist

logging cdg_virtualIP
logging on
logging buffered 307200-125000000

logging source-interface interface_name

logging trap informational
logging events level informational
logging events link-status
logging events link-status software-interfaces

no cli whitespace completion
domain ipv4 host server_name cdg_virtualIP
```

Set up VTY options:

```
line default
exec-timeout 10
session-limit 10
session-timeout 100
transport input all
transport output all
vty-pool default 0 99 line-template default
```

TELNET and SSH Settings:

```
telnet ipv4 server max-servers no-limit
telnet vrf default ipv4 server max-servers 100
```

```
ssh server v2
ssh server rate-limit 60
cinetd rate-limit 60
```

Configure the NetConf and XML agents:

```
xml agent tty
netconf agent tty
```

Monitor device with Virtual IP address :

```
ipv4 virtual address use-as-src-addr
ipv4 virtual address Virtual_IP_Address/Subnet_Mask
```

Enable CFM modeling:

```
snmp-server view all 1.3.111.2.802.1.1.8 included
```

For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO SystemOwner
```

For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha encrypted Password priv des56 encrypted
Password SystemOwner
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group
snmp-server group Group v3 priv read v1default write v1default notify v1default
```

Configure the following to improve the SNMP interface stats response time:

```
snmp-server ifmib stats cache
```

Configure SNMP traps for physical interfaces to ensure that link-down scenarios are captured:

```
snmp-server interface subset 2 regular-expression Forty*
notification linkupdown
!
snmp-server interface subset 3 regular-expression Ten*
notification linkupdown
!
snmp-server interface subset 1 regular-expression Hun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression TwoHun*
notification linkupdown
!
snmp-server interface subset 1 regular-expression FourHun*
notification linkupdown
```

Enable SNMP entity field replaceable unit (FRU) control traps:

```
snmp-server traps fru-ctrl
```

Syslogs are used by Crosswork Network Controller for alarm and event management. NTP settings ensure that Crosswork Network Controller receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
logging facility local7
logging cdg_virtualIP vrf name
```

For Cisco ASR 9000 Series devices operating as Large Routers (LRs), configure gNMI using these commands:

```
GNMI Configuration

grpc
 port <port no>
!
```

Configuration sample for Cisco IOS-XE devices

These commands provide a sample pre-onboarding device configuration for IOS-XE devices.

```
snmp-server host cdg_virtualIP
snmp-server community public-cmty RO
snmp-server community private-cmty RW
snmp-server ifindex persist

logging cdg_virtualIP
logging on
logging buffered 64000 informational

logging source-interface interface_name
logging trap informational
logging event link-status default
```

Disable domain lookups to avoid delay in TELNET/ SSH command response:

```
no ip domain-lookup
```

Enable SSH

```
crypto key generate rsa
ip ssh rsa keypair-name keypair-name
crypto key generate rsa usage-keys label key-label modulus modulus-size
ip ssh version [1 | 2]
```

Setup VTY options:

```
line vty <number of vty>
exec-timeout
session-timeout
transport input all
transport output all
```

For SNMPv2 only, configure the community string:

```
snmp-server community ReadonlyCommunityName RO
```

For SNMPv3 only, configure the following settings:

```
snmp-server user User Group v3 auth sha Password priv des Password
snmp-server view Group 1.3.6 included
snmp-server view Group 1.0.8802.1.1.2 included
snmp-server group Group v3 priv notify Group read Group

snmp-server group Group v3 priv read v1default write v1default notify v1default
snmp-server group Group v3 priv
snmp-server group Group v3 priv notify crosswork read crosswork
```

Configure the cache settings at a global level to improve the SNMP interface response time using the configuration:

```
snmp-server cache
```

Syslogs are used by the Crosswork Network Controller for alarm and event management. NTP settings ensure that Crosswork Network Controller receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
service timestamps log datetime show-timezone msec year
ntp server NTP_Server
update-calendar
logging facility local7
logging cdg_virtualIP vrf default severity info [port default]
```

Configuration sample for Cisco NSO devices

These commands provide a sample pre-onboarding configuration for a Cisco NSO device used as provider to configure devices managed by Crosswork Network Controller.

This example shows a Cisco NSO configuration that uses the hostname as the device ID. If you are using a CSV file to import devices, use **ROBOT_PROVDEVKEY_HOST_NAME** as the enum value for the provider_node_key field. The example hostname **RouterFremont** used here must match the hostname for the device in the CSV file.

```
configure
set devices device RouterFremont address 198.18.1.11 port 22
```

In the following example, we are creating an authgroup called "cisco", with a remote name and password of "cisco". Next, we are setting all the devices that have a name starting with "Router" to a device type of "netconf" using the ned-id "cisco-iosxr-nc-6.6". Finally, we are assigning all of the devices with a name starting with "Router" to the "cisco" authgroup. Edit these settings to match your environment:

```
set devices authgroups group cisco default-map remote-name cisco remote-password cisco
set devices device Router* device-type netconf ned-id cisco-iosxr-nc-6.6
set devices device Router* authgroup cisco
```

The following CLI commands unlock and retrieve the SSH keys from all of the devices. Cisco NSO synchronizes itself with the devices by uploading each device's current configuration and then storing the present configuration. It is important to use these commands to ensure that the devices, Cisco NSO, and your Cisco Crosswork applications are starting from a common configuration:

```
set devices device Router* state admin-state unlocked
request devices device Router* ssh fetch-host-keys
request devices device Router* sync-from
commit
```

Configuration sample for Nexus devices

These commands provide a sample pre-onboarding device configuration for Nexus devices that sets the correct SNMPv2 and NETCONF configuration, and SSH rate limits. The NETCONF setting is only needed if the device is MDT-capable.

```
logging console 7
logging monitor 7
!
ntp server <NTPServerIPAddress>
ntp server <10.10.10.11> use-vrf <management or configured vrf>.
!
ssh idle-timeout
logging level security
```

```
!
feature netconf
feature openconfig
!
snmp-server user <User>  auth md5 <String> priv aes-256 <String>
!
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp

snmp-server community community_name RO
!
logging server <IP>
logging source-interface interface_name
logging event link-status default
logging event link-status enable
```

- User privileges can be configured as either `network-admin` or `network-operator`
- In Nexus OS, the ifIndex for an interface is persistent.
- To retrieve the SNMP interface index (ifmib index), use the following command:

  ```
  show interface snmp-index
  ```

- To configure logging for link status or trunk status changes, use the following command in configuration mode:

  ```
  logging event link-status default
  logging event link-status enable
  ```

Set up VTY options:

```
line vty
exec-timeout 10
session-limit 10
```

Forward events to the Crosswork Network Controller server using the snmp-server host command:

```
snmp-server host <192.168.90.135> traps version 2c public udp-port 1062
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps link linkDown
snmp-server enable traps link linkUp
```

Configure the following to improve the SNMP interface stats response time:

```
snmp-server counter cache enable
snmp-server counter cache timeout <1-3600>
```

Enable SNMP entity field replaceable unit (FRU) control traps:

```
snmp-server enable traps entity
```

Syslogs are used by Crosswork Network Controller for alarm and event management. NTP settings ensure that Crosswork Network Controller receives the correct timestamps for events. To configure syslogs on the device, add the following settings:

```
clock timezone TimeZone
ntp server NTP_Server
logging level ntp 7
logging server <IP> use-vrf <vrf name>
```

The `service timestamps` feature is not supported in Nexus OS. To set the logging level for a specific facility (e.g., NTP), use the following command:

```
logging level ntp 7
```

Configuration sample for gNMI and gRPC

These commands provide a sample pre-onboarding configuration for a device to enable telemetry using gNMI and gRPC.

```
grpc
vrf mgmt
port 57500
no-tls
max-streams 128
max-streams-per-user 128
address-family dual
max-request-total 256
max-request-per-user 32
!

tpa
vrf mgmt
  address-family ipv4
   default-route mgmt
  !
  address-family ipv6
   default-route mgmt
  !
!
!
```

gNMI bundling configuration for ASR 9000 series Large Routers

Enabling gNMI bundling is recommended for Cisco ASR 9000 Series devices configured as Large Routers. For inventory collection, gNMI bundling is mandatory to meet requirements. Bundling groups multiple gNMI updates into a single update, which is crucial for inventory collection on high-scale devices.

Sample configuration for gNMI bundling:

```
telemetry model-driven
 gnmi
  bundling
   size 65536
  !
 !
!
```

Configuration sample for IGP protocol router ID

These commands provide a sample pre-onboarding device configuration for ISIS and OSPF.

ISIS router ID:

```
router isis 1
 net 49.0010.0100.0004.00
 distribute link-state instance-id 100
 log adjacency changes
 affinity-map top bit-position 101
 affinity-map bottom bit-position 102
 address-family ipv4 unicast
  metric-style wide
  mpls traffic-eng level-2-only
  mpls traffic-eng router-id Loopback0
  router-id 198.19.1.4
  segment-routing mpls
#show mpls traffic-eng igp-areas
Fri Oct  4 03:53:16.117 UTC
```

```
MPLS-TE IGP Areas

Global router-id:         198.19.1.4
Global optical router-id: Not available

IS-IS 1

    IGP ID:                      0010.0100.0004
    TE router ID configured:     198.19.1.4
                 in use:         198.19.1.4
    Connection:                  up
```

OSPF router ID:

```
router ospf
 distribute link-state instance-id 6
 router-id 1.1.1.20
 segment-routing global-block 16000 17999
 segment-routing forwarding mpls
 segment-routing sr-prefer
#show mpls traffic-eng igp-areas
Fri Oct  4 03:53:28.091 UTC

MPLS-TE IGP Areas

Global router-id:         1.1.1.20
Global optical router-id: Not available

OSPF

    IGP ID:                      1.1.1.20
    TE router ID configured:     1.1.1.20
                 in use:         1.1.1.20
    Connection:                  up
```

Configuration sample for MDT sensor group

These commands provide a sample pre-onboarding configuration for a device to stream telemetry data.

```
telemetry model-driven
!
destination-group Crosswork
  vrf mgmt
  address-family ipv4 x.x.x.x port 9010
   encoding self-describing-gpb
   protocol tcp
  !
sensor-group Crosswork
  sensor-path Cisco-IOS-XR-infra-tc-oper:traffic-collector/afs/af/counters/tunnels/tunnel
!
subscription Crosswork
  sensor-group-id Crosswork
  destination-id Crosswork
!
!
```

Configuration sample for SNMPv2 and SNMPv3 traps

These commands provide a sample configuration for a device to send SNMP traps.

For SNMP v2 traps:

```
snmp-server trap link ietf
snmp-server host cdg_virtualIP traps version 2c Community String udp-port 1062
snmp-server community Community String
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
```

For SNMP v3 traps:

```
snmp-server trap link ietf
snmp-server host cdg_virtualIP traps version 3 Community String udp-port 1062
snmp-server community Community String
snmp-server traps snmp linkup
snmp-server traps snmp linkdown
```

Configuration sample for SNMPv3 data collection

These commands provide a sample configuration for SNMPv3 data collection. These commands must be added in addition to the SNMPv2 commands referenced in the section, Configuration sample for SNMPv2 and SNMPv3 traps, on page 308.

```
snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 password priv aes 128 password
```

Add devices individually through the UI

Add devices one by one using the user interface, best suited when adding only a few devices.

Before you begin

Gather the required device details, such as name, IP address, and authentication credentials.

Follow these steps to add a device individually through the UI:

Procedure

Step 1 From the main menu, choose **Device Management** > **Network Devices**.

Step 2 Click the add icon.

Step 3 Enter the values for the new device, as listed in Field descriptions for new device addition, on page 309.

Step 4 Save your changes.

Step 5 (Optional) Repeat these steps to add more devices.

Field descriptions for new device addition

This table lists the fields available when adding a new device through the Crosswork Network Controller user interface, along with each field's description.

Attention Starting from version 7.1, the **Device type** field is deprecated in Crosswork Network Controller.

Table 41: Fields in the Add new device window (=Required)*

Field	Description
Device information	
*** Admin state**	The management state of the device. Options are • **UNMANAGED**—Crosswork Network Controller is not monitoring the device. • **DOWN**—The device is being managed and is down. • **UP**—The device is being managed and is up.
*** Reachability check**	Determines whether Crosswork Network Controller performs reachability checks on the device. Options are: • **ENABLE** (In CSV: **REACH_CHECK_ENABLE**)—Checks for reachability and then updates the Reachability State in the user interface automatically. • **DISABLE** (In CSV: **REACH_CHECK_DISABLE**)—The device reachability check is disabled. Cisco recommends that you always set this to **ENABLE**. This field is optional if **Configured State** is marked as **UNMANAGED**.
Serial number	Serial number for the device.
Host name	The hostname of the device.
Tags	The available tags to assign to the device for identification and grouping purposes. Use device tags to group devices for monitoring, and to provide additional information that might be of interest to other users, such as the device's physical location or its administrator's email ID. **Attention** When onboarding Cisco ASR 9000 Large Routers, you must first create the **large-interface-density** tag under the **DeviceClassification** category and subsequently apply this tag to the devices.
Software type	Software type of the device. **Note** Some third-party vendor devices require a specific string to be entered as part of the **Software Type** field. These are the required strings for different vendors: • Juniper devices: JUNOS • Huawei devices: VRP • Nokia devices: TIMOS
Software version	Software version of the operating system.
UUID	Universally unique identifier (UUID) for the device.
MAC address	MAC address of the device.

Field	Description
Inventory ID	Inventory ID value for the device. The value can contain a maximum of 128 alphanumeric characters, and can include dots (.), underscores ("_"), colons (":"), or hyphens ("-"). No other special characters are allowed. Choose the device host name or an easily identifiable name for Inventory ID as this will be used to sync the device to Crosswork Network Controller with the Inventory ID used as the device name.
Product type	Product type of the device. **Note** For unsupported devices, Crosswork Network Controller reports Manufacturer[sysoid] in the **Product type** column. In cases where unsupported devices do not comply with SNMPv2 MIB, the **Product type** might not show data or may display incorrect data.
Syslog format	The format in which syslog events received from the device should be parsed by the syslog collector. The options are: • **UNKNOWN** - Choose this option if you are uncertain or if you do not want any parsing to be done by the syslog collector. The Syslog Collection Job output contains syslog events as received from the device. • **RFC5424** - Choose this option to parse syslog events received from the device in RFC5424 format. • **RFC3164** - Choose this option to parse syslog events received from the device in RFC3164 format. Refer to Section: Syslog Collection Job Output for more details
CLI cache enabled	Click the checkbox if you wish to enable CLI cache.
Connectivity details	
*** Credential Profile**	The name of the credential profile to be used to access the device for data collection and configuration changes. Select the profile for which the device is configured from the dropdown list. For example: **nso23** or **srpce123**. This field is optional if **Administration State** is marked as **UNMANAGED**.
Protocol	The connectivity protocols used by the device. Choices are: **SNMP**, **NETCONF**, **TELNET**,**HTTP**, **HTTPS**, **GNMI**, **TL1**, and **GRPC**. **Note** Toggle the **Secure Connection** slider to secure the GNMI protocol that you have selected. In this documentation, the secured gNMI protocol is referred to as GNMI_Secure. To add more connectivity protocols for this device, click the add icon at the end of the first row in the **Connectivity Details** panel. To delete a protocol you have entered, click the cross icon shown next to that row in the panel. You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol. Enter details for at least **SSH** and **SNMP**. If you do not configure **SNMP**, the device will not be added. If you want to manage the device (or you are managing XR devices), you must enter details for **NETCONF**. TELNET connectivity is optional.

Field	Description
*** IP Address / Subnet Mask**	Enter the device's IP address (IPv4 or IPv6) and subnet mask. **Note** If you have multiple protocols with the same IP address and subnet mask, you can instruct Crosswork Network Controller to autofill the details in the other fields. **Note** Please ensure that the subnets chosen for the IP networks (including devices and destinations) do not have overlapping address space (subnets/supernets) as it may result in unpredictable connectivity issues.
*** Port**	The port used for this connectivity protocol. For each protocol enabled on the device, the default port is automatically provided. This default value works correctly in most cases. However, if your network uses non-standard ports, you must update the port settings to match the ones configured in your network. GNMI and GNMI_SECURE: When using gNMI the value is not automatically populated. You must instead enter the value configured on your network devices. The port values range between 57344 to 57999. Ensure that the port number you enter here matches with the port number configured on the device.
Timeout	The elapsed time (in seconds) before communication attempts using this protocol times out. The default value is 30 seconds. While the default value is 30 seconds, a minimum timeout value of 90 seconds is recommended for XE devices using NETCONF. For all other devices and protocols, the recommended minimum timeout value is 60 seconds.
Encoding Type	This field is only applicable for **GNMI** and **GNMI_SECURE** protocols. The options are **`JSON`**, **`BYTES`**, **`PROTO`**, **`ASCII`**, and **`JSON IETF`**. Based on device capability, only one encoding format is supported at a time in a device.
Encryption	This field is applicable only to the SNMP protocol. From the drop-down list, choose the appropriate SNMPv3 protocol supported by the device. The default value is NONE. The drop-down list presents several Advanced Encryption Standard (AES) options, including Counter mode (CTR), Galois/Counter mode (GCM), and Cipher Block Chaining mode (CBC), each supporting various key lengths (128-bit, 192-bit, and 256-bit). The credential profile supports the generic privacy types such as AES-192 and AES-256. For Cisco devices, these are specified as CiscoAES192 and CiscoAES256 protocols. On Cisco devices, the protocols appear as aes256-ctr, aes256-gcm@openssh.com, aes256-cbc, aes192-ctr, and aes192-cbc. To ensure compatibility with Crosswork Network Controller polling, Cisco devices must use these updated protocol variations. On non-Cisco devices, select the encryption that the device supports or use NONE if the device does not use encryption for SNMP.

Field	Description
Trap source IP	This field is available only when the SNMP protocol is selected. Use this field to specify the source IP address that the device will use to report SNMP traps if it differs from the default management interface IP address. For consistent trap collection, ensure that the IP address entered in the **Trap source IP** field matches the `trap-source` parameter configured on the network device to avoid any issues with SNMP trap handling. **Note** • If the **Trap source IP** field is not specified, Crosswork Network Controller defaults to using the management interface IP address. For devices added via CSV or API, this field also defaults to the management interface IP address unless explicitly specified. • Ensure that the trap source uses the same IP stack (IPv4 or IPv6) as the device connectivity protocol to maintain consistent communication and avoid mismatches.
SNMP Disable Trap Check	This check box appears when the protocol field is set to **SNMP**. Selecting this check box disables the SNMPv2 community string validation between the network device and Data Gateway. Disabling the SNMPv2 community string validation might be a requirement when you want to use a different community string for traps than the one in the credential profile.
*** Capability**	The capabilities that allow collection of device data and that are configured on the device. You must select at least **SNMP** as this is a required capability. The device will not be onboarded if **SNMP** is not configured. Other options are **YANG_MDT**, **YANG_CLI**, **TL1**, and **GNMI**. The capabilities that you select will depend on the device software type and version. **Note** • For devices with MDT capability, do not select **YANG_MDT** at this stage. • To enable Crosswork Network Controller to receive the syslog-based data, select **YANG_CLI**.
Providers and access Provide the provider information.	
Provider family	Provider type used for topology computation. Choose a provider from the list.
Provider name	Provider name used for topology computation. Choose a provider from the list. **Note** For Cisco NSO LSA deployment, select the resource-facing service (RFS) node to which you want to assign the device.
Credential	The credential profile used for the provider. This field is read-only and is autopopulated based on the provider you select.
Device key	The hostname used to link this device record to its corresponding record on the provider. This is typically the device's full hostname, including the domain.
Routing info	

Field	Description
ISIS system ID	The device's IS-IS system ID. This ID identifies the router in an IS-IS topology, and is required for SR-PCE integration. This field is a configurable parameter, and cannot be autodiscovered by Crosswork Network Controller.
OSPF router ID	The device's OSPF router ID. This ID identifies the router in an OSPF topology, and is required for SR-PCE integration. This field is a configurable parameter, and cannot be autodiscovered by Crosswork Network Controller.
***TE router ID**	The traffic engineering router ID for the respective IGP. **Note** For visualizing L3 links in topology, devices should be onboarded to Crosswork Network Controller with the **TE Router ID** field populated.
IPv6 router ID	IPv6 router ID for the device. This field is a configurable parameter, and cannot be autodiscovered by Crosswork Network Controller.
Streaming telemetry config	
VRF	Name of the VRF within which Model Driven Telemetry (MDT) traffic is routed.
Source interface	The range of loopback address for the device type. This field is optional. However, we recommend specifying the loopback associated with the VRF by using the selector in the adjacent box. **Note** This field can be edited only when the device is in a DOWN or UNMANAGED state.
Opt out MDT config	When enabled, Crosswork Network Controller will not push telemetry configuration to the device via NSO. The default setting state is Disabled (which allows Crosswork Network Controller to push telemetry configuration to the device via NSO). The device must be in ADMIN DOWN state to toggle this setting. Any out of band configuration setup must be cleared before moving the setting from Enabled to Disabled.
Location Provide location information if you want to see your devices on the geographical map.	
Building	Enter the name of the building.
Street	Enter the name of the street.
City	Enter the name of the city.
State	Enter the name of the state.
Country	Enter the name of the country.
Region	Enter the name of the region.
Zip	Enter the zip code of the region.

Field	Description
Longitude	Longitude value is required so that the geographical map can present the correct geographical location of the device and its links to other devices. Enter the longitude in Decimal Degrees (DD) format.
Latitude	Latitude value is required so that the geographical map can present the correct geographical location of the device and its links to other devices. Enter the latitude in Decimal Degrees (DD) format.
Altitude	The altitude at which the device is located. If you do not know the altitude or do not wish to track it, you can leave this field blank. Alternatively, you may use this field to specify the floor of the building where the device is installed. The value must be a numeric entry.

CSV device imports

A CSV device import is a bulk onboarding method that:

- enables users to add multiple devices to the Crosswork Network Controller in a single action,
- allows avoidance of repetitive manual entry, and
- updates existing records when matching inventory key types are found (excluding system-generated UUIDs).

CSV import is most useful in large environments where device addition efficiency and accuracy are critical.

CSV file behavior

- Import only adds devices not already present in the database.
- Existing device records (excluding system-generated UUIDs) are overwritten if the inventory key type matches a record in the CSV.
- Fields requiring unique values, such as VRF, router loopback, or loopback ID, must be explicitly set.
- Non-required fields can be left blank, set to a default value, or are auto-populated after device communication is established (e.g., model, type, software version).

Handling non-required fields in the CSV file

For fields that are not required in the CSV, the following can occur:

- The field may be left blank.
- The field may be set to a default value.
- The field may be populated with values retrieved from the device once communication is established, such as model, type, or software version.

Recommendations for CSV import

To prevent errors when importing CSV files, follow these recommendations:

- Export a backup copy of your existing device list before any CSV import, to prevent accidental data loss.
- Export the current device configuration to generate a CSV template tailored to your environment. Use this exported file as a baseline for further additions.
- Always make necessary edits to exported CSV files. Files exported directly from the UI cannot be re-imported without changes.
- Add a few devices using the Crosswork Network Controller UI and verify they are functioning before importing in bulk.
- Before importing, ensure the Crosswork Data Gateway and UUID columns in the CSV file are empty.
- If importing multiple CSV files, verify that there are no duplicate devices between them.
- If there are any errors in the import file, they are not reported all at once. Instead, the system identifies and displays errors one at a time, starting with the first error it encounters. Address these errors sequentially as reported during import.
- The device import CSV format differs for cluster deployments versus single VM deployments. Use the correct template for your environment.

Formatting guidelines

- CSV files from Windows machines must use ‘newline’ characters, not ‘carriage return,’ in order to process correctly.
- To enter multiple values in a field, use semicolons (e.g., SSH;SNMP;NETCONF). Use double semicolons ‘;;’ with no space for blank fields.
- Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank. When you separate multiple entries with semicolons, remember that the order in which you enter values in each field is important.

  For example, if you enter `SSH;SNMP;NETCONF` in the **Connectivity Type** field and you enter `22;161;830` in the **Connectivity Port** field, the order of entry determines the mapping between the two fields:

  - SSH: port 22
  - SNMP: port 161
  - NETCONF: port 830

Template usage

After downloading and editing the CSV template, delete all sample data rows before saving. Retain only the column header row for import.

Special fields

Populate the TE router ID for each device to ensure unique identification within the topology.

Device reachability

Devices may initially show as unreachable or not operational when they are first imported. However, if they are still displayed as unreachable or not operational after 30 minutes, there may be an issue that needs to be investigated. To investigate, select **Device Management** > **Job History** and click on any error icon you see in the **Status** column. Common issues include failure to ensure the associated credential profile contains the correct credentials. You can test this by opening a terminal window on the server and then trying to access the device using the protocol and credentials specified in the associated credential profile.

Add devices from a CSV file

Add multiple network devices to Crosswork Network Controller by importing their details from a CSV file.

Use this task when you want to onboard several devices at once, rather than adding them individually.

Procedure

Step 1 Choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed.

Step 2 Open the **Import CSV File** dialog box.

Step 3 If you have not already created a device CSV file to import:

a) Click the **Download sample 'Device Management template (*.csv)' file** link and save the CSV file template to a local storage resource.

b) Open the template using your preferred tool. Begin adding rows to the file, one row for each device.

c) Delete the sample data rows before saving the file, or they will be imported along with your data. You can keep the column header row, as it is ignored during the import process.

d) Save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you created in the previous steps and then click **Open** to select it.

Step 5 With the CSV file selected, click **Import** and wait for the import to complete.

Step 6 Resolve any errors and confirm device reachability.

Step 7 Once you have successfully onboarded the devices, map them to a data gateway instance.

Export device information to a CSV file

Keep a record of all devices in the system at one time by exporting the device information.

You can also edit the CSV file as needed, and re-import it to overwrite existing device data.

Procedure

Step 1 From the main menu, choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed by default.

Step 2 (Optional) Filter the device list as needed.

Step 3 Check the check boxes for the devices you want to export.

Step 4 Click .

Large Routers

A Large Router (LR) is a high-scale ASR 9000 router category that

- supports very large interface counts,
- requires a specialized inventory collection approach for reliable discovery, and
- is identified by Crosswork Network Controller to enable optimized inventory handling.

Some ASR 9000 router deployments operate at significantly higher interface scale than typical devices. At this scale, standard inventory collection approaches are not sufficient. Crosswork Network Controller introduces the LR classification to distinguish these high-scale ASR 9000 routers and apply an inventory strategy suited to large-scale deployments, without affecting inventory behavior for other devices.

Requirements for LR inventory

This section describes the device-side requirements and inventory behavior that must be met before onboarding a LR in Crosswork Network Controller.

Criteria for LR inventory support

Large router inventory support applies only to devices that meet all these conditions:

Table 42: Criteria for LR inventory support

Attribute	Value
Platform	ASR 9000 (ASR 9K)
Minimum number of interfaces	1000
Software version	Special image- *Contact Cisco Customer Experience*
Supported scale	Up to 48K interfaces
GNMI encoding	JSON_IETF encoding

Devices that do not meet these criteria are not supported for LR inventory handling.

GNMI configuration requirements

Inventory collection for LR uses GNMI.

Ensure these configurations on the ASR 9K device:

- GNMI is enabled on the device
- GNMI access is available using the configured device credentials

- GNMI supports the OpenConfig interfaces model

GNMI-based inventory collection is triggered during device addition and inventory synchronization.

For GNMI configuration sample, see Configuration sample for gNMI and gRPC, on page 307.

GNMI bundling requirements

GNMI bundling is **recommended** on ASR 9K devices used as LRs to improve inventory performance. Bundling groups multiple GNMI updates into a single update, reducing processing overhead.

For LR devices:

- Inventory relies on bundled GNMI responses to complete collection efficiently.
- If GNMI bundling is not enabled, inventory collection may fail.

Inventory collection behavior

For devices that meet the LR criteria:

- Inventory uses GNMI with **JSON_IETF** encoding
- CLI- and SNMP-based interface collection is bypassed only for the inventory features that have been replaced by GNMI-based large routers collection.

Onboard large ASR 9000 routers

Onboard an ASR 9000 Large Router device to enable large-scale inventory collection of interface data through GNMI.

Onboarding the ASR 9000 LR ensures that all interface and sub-interface information from the device is accessible in the inventory system. This is required for comprehensive monitoring and management of large wireless routers within your network, especially when using GNMI for scalable data retrieval.

Note GRE tunnel interfaces are not modeled in inventory for LR devices.

Before you begin

Ensure that the device meet the requirements mentioned in Requirements for LR inventory, on page 318.

Follow these steps to onboard an LR device:

Procedure

Step 1 Create the LR identification tag (one-time setup).

For information on tag creation, see Create tags, on page 292.

- **Category**: `DeviceClassification`
- **Tag name**: `large-interface-density`

Note
This tag is not created by default and must be manually created.

Step 2 Create a credential profile that includes GNMI credentials, SNMP credentials, and CLI credentials.

For more information, see Create credential profiles, on page 240.

Step 3 Add a new ASR 9K device. For more information, see Add devices individually through the UI, on page 309 and Field descriptions for new device addition, on page 309.

- Set **Admin state** to **Up**.
- Enable **Reachability check** (recommended).
- Select **Tag** as `large-interface-density`.
- Select the credential profile created earlier.

Note
If the `large-interface-density` tag is applied to an unsupported device, inventory collection will not complete.

Step 4 Add the newly added device to a Data Gateway.

For more information, see Attach devices to Data Gateway, on page 75.

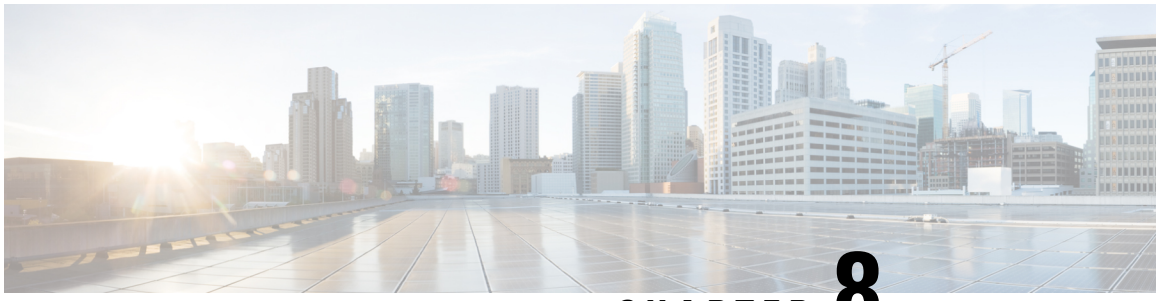
Note
Distribute LR devices evenly across available Data Gateways to avoid overloading a single gateway.

Step 5 Trigger inventory synchronization.

a) On the **Network Devices** window, perform an inventory sync.
   - Select the ASR 9000 devices and click **Actions** > **Detailed sync selected devices**.
   - If you do not select any devices, click **Actions** > **Detailed sync all devices**.

b) Monitor the device status.
   - Status changes to **In progress**
   - On success, status changes to **Completed**

- The device reaches **Completed** state.
- All interfaces are visible under the **Interfaces** tab, which can be accessed by navigating to **Topology** > **Device details** or **Topology** > **Device details** > **Detailed inventory**.



CHAPTER 8

Topology map for network visualisation

Topology maps

A topology map is a network visualization tool that

- displays network devices and their connections using logical or geographical layouts,
- allows you to filter, group, and interact with devices and links for better analysis, and
- integrates device inventory data to provide real-time status, alarm, and performance insights.

For information on managing your devices and inventory, viewing interface details, and performing actions such as inventory synchronization, refer to the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management* guide.

Prerequisites

- Devices must be onboarded to the system before using the topology map. See Device onboarding methods.

  All devices in the network must have single-topology settings configured before you onboard the topology. Configuring single-topology on only some devices is not supported and will cause links to appear as degraded or missing. Changing devices from non-single-topology to single-topology or the other way round after onboarding is also not supported. In single-topology mode, note that only the IPv4 metric is used, even if you configure IPv6 metrics.

Topology map views

Topology maps support two main views:

- Logical map: Arranges devices and links based on user-modifiable algorithms, irrespective of their physical location.
- Geographical map: Plots devices, clusters, links, and tunnels on a world map using GPS coordinates from the device inventory.

Filtering topology

- Filter your view by creating device groups.
- Display devices and links by selected network layers.
- Save custom views to retain filter and display settings across sessions.

Link representation and details

- Solid line: Represents a single physical or logical link between two devices.
- Dashed line: Represents an aggregated link, which may include multiple Layer 2 links (for example, several Ethernet links) or multiple Layer 3 links (such as multiple ISIS connections) over the same physical link.
- Color links to quickly identify status, such as link down, or utilization level.
- “A” and “Z” labels indicate the interfaces connecting links between devices.
- To view details for a link, click the link to open the **Links** panel, which shows information on the right side of the interface.

Topology map UI elements

The table describes key UI elements and actions on the topology map:

Feature/Action	Description
Topology map view	Choose views such as Topology, Traffic Engineering, VPN Services, or Transport Slicing from the **Show** drop-down.
Device groups	Filter displayed devices by group.
Show layers	Display devices and links belonging to selected network layers.
Topology map	View devices and links with options to drill down for detailed device or link information.
Map type selector	Switch between logical and geographical maps.
Side panel controls	Expand, collapse, or hide the side panel for more map viewing area.
Mini dashboard	Monitor IP Domain, device reachability and alarm severity.
Contextual panel	See information relevant to the selected device, link, or policy depending on installed applications.
Saved views	Create and recall named custom views of the map along with table settings and filters.

Upload internal map files for offline use

Enable detailed geographical map display within the Crosswork Network Controller when there is no internet connection to Mapbox or other external map providers.

Note If you choose to work offline with internal maps and you do not upload map files, your geographical map will display as a generic world map without details of cities, streets, and so on.

By default, the system retrieves map tiles from an external provider. If your environment lacks Internet connectivity, you can upload Cisco-provided internal map files to ensure geographical features are displayed accurately. Upload only those map files that are relevant to your network's regions. If no map files are uploaded, only a generic, less-detailed world map will be shown.

Before you begin

- Ensure you can access Cisco.com to download the required signed map files.
- Verify you have credentials and permissions to upload files in Crosswork Network Controller.

Procedure

Step 1 Download the map file from Cisco.com.

a) Go to Cisco Software Download Center and download the signed map file for your region to your local computer.

Example file name: `signed-us-geomaps-1.0.0-for-Crosswork-7.0.0.tar.gz`

b) Open a terminal or file explorer and extract the `.tar.gz` file.

Example:

```
cd <folder where tar was downloaded>
tar -xvf signed-us-geomaps-1.0.0-for-Crosswork-7.0.0.tar.gz

README
us-geomaps-1.0.0-for-Crosswork-7.0.0-signed.tar.gz
us-geomaps-1.0.0-for-Crosswork-7.0.0-signed.tar.gz.signature
cisco_x509_verify_release.py
cisco_x509_verify_release.py3
CW-CCO_RELEASE.cer
```

Step 2 Upload the extracted map file into Crosswork Network Controller.

a) In Crosswork Network Controller, go to **Administration** > **Settings** > **System settings**.
b) Under **Topology**, select **Map**.
c) Select the **Work offline with internal maps** and then click **Manage**.
d) In the **Manage internal maps** dialog, click the upload icon to add a new map file, one at a time.
e) Browse to the location of the extracted `.signed.tar.gz` file, select it, and click **Upload**.

Example: `us-geomaps-1.0.0-for-Crosswork-7.0.0-signed.tar.gz`

The selected regional map is available for offline geographical display. When working offline, the Controller now shows detailed maps based on the uploaded files, improving network visualization.

What to do next

- If you manage networks across multiple regions, repeat the process for each relevant map file.
- Confirm correct map display on the geographical interface.

Device groups

A device group is a device category that

- organizes devices into logical collections based on user-defined criteria,
- enables filtering and visualization of data from specific sets of devices, and
- simplifies monitoring by reducing screen clutter and focusing attention on relevant device data.

Create device groups

Organize devices into groups to simplify management, policy assignment, and bulk operations within your network platform.

Device groups let you manage related devices together. You can create groups manually or set up automatic grouping rules (see Create rule for dynamic device grouping). Note that each device can belong to only one device group.

Procedure

Step 1 From the main menu choose **Device Management** > **Device Groups**. We see that a device group has been selected. Also note that only the devices belonging to that device group are listed in the devices table in the right pane.

Step 2 To create a new sub-group, select the parent group and choose **Add a sub-group**.

Step 3 Enter the required details for the sub-group and select **Create**.
The new sub-group appears under the selected parent device group.

Create dynamic device group rules

Automatically organize unassigned devices into dynamic groups using rules based on device host names or IP addresses.

You can create a rule to dynamically create device groups and automatically add unassigned devices to these groups using a Regular Expression (regex) on the device host name or IP address.

Before you begin

Dynamic rules do not apply to devices that already belong to groups. Move devices already in other groups to "Unassigned Devices" if you want the rule to apply to them.

Procedure

Step 1 From the main menu choose **Device Management** > **Device Groups**.

Step 2 Click next to **All Locations > Manage Location Dynamic Groups**.

Step 3 Click **Show more details and examples** to help you fill out the required host name or IP address.

Step 4 If there are any existing devices in the **Unassigned Devices** group, test your rule to preview potential group assignments.

Step 5 Enable the rule to start automatically assigning matching unassigned devices to dynamic groups.

The system checks for unassigned devices every minute and applies your rule.

Step 6 Save your changes.

Step 7 Review the newly created groups under **Unassigned Groups** and move groups into your preferred hierarchy as needed.

Unassigned devices matching your rule criteria are automatically placed into the correct dynamic groups.

Modify device group details

Change the name, parent group, or description of an existing device group to keep your network structure up to date.

Modify device groups when reorganizing devices or updating administrative records.

Procedure

Step 1 From the main menu choose **Device Management** > **Device Groups**.

Step 2 Select the device group you want to update.

Step 3 Edit the group details, and description as needed.

Step 4 Save your changes.

Delete a device group

Remove an existing device group and make its devices available for assignment to other groups.

Use this task when you need to delete a device group that is no longer required. Deleting a group will unassign all devices from that group, and make them available for reassignment.

Before you begin

Procedure

Step 1 From the main menu choose **Device Management** > **Device Groups**.
Step 2 Select the device group you want to delete.
Step 3 Open the actions menu for the group and choose **Delete group**.
Step 4 In the confirmation dialog, click **Delete** to confirm and complete the deletion.

The device group is deleted, and its devices are unassigned and available for reassignment to other groups.

Move devices from one group to another

Transfer devices to a different group to reorganize network assets and adjust policies or administrative boundaries as needed.

Use this task to efficiently regroup devices. This is useful during organizational changes, policy updates, or network scaling.

Before you begin

Identify the devices and the target group for the transfer.

Procedure

Step 1 From the main menu choose **Device Management** > **Device Groups** .
Step 2 Select the source group from which you wish to move the devices.
Step 3 Select the devices to transfer.
Step 4 Click **Move**, then choose the target group from the drop-down and confirm.

If devices do not appear on device maps after moving, update your display settings:

- Go to **Administration > Settings**, then click the **User settings** tab.
- Options include:
  - **Automatically switch to the device group that will show all participating devices** - Ensures all relevant devices for a service or policy are shown.
  - **Don't switch the device group automatically** - Keeps your current device group selection, even if all devices are not shown.
  - **Ask me each time** - Prompts you when a device could be missing from the map.

The devices are now part of the new group and visible in the target group's listing.

Import multiple device groups

Import multiple device groups at once and update existing ones in bulk by uploading a CSV file.

When you import device groups from a CSV file, new device groups are created for entries not already in the database. Existing groups are updated if the imported data matches them.

Importing device groups may overwrite current data, so exporting a backup of current device groups before importing is recommended.

Before you begin

- Prepare a CSV file containing your device group data, using the provided template format.
- Back up your current device groups to prevent accidental data loss.

Procedure

Step 1 From the main menu, choose **Device Management** > **Device Groups** .

Step 2 Click **Import groups** to open the dialog box.

Step 3 If you have not prepared a device groups CSV file:

a) Download the device groups CSV template to a local storage resource.

b) Open the template in your preferred editor and add one row for each device group.

Use a semicolon to separate multiple entries in the same field. Use two semicolons with no space between them to indicate that you are leaving the field blank.

c) Remove all sample data rows, leaving only the column header row.

d) When you are finished, save the new CSV file.

Step 4 Click **Browse** and select your completed CSV file.

Step 5 With the CSV file selected, click **Import** .

Note
Wait for the import to complete before clicking Import again to avoid duplicate device group entries.

The selected device groups are imported and updated as needed.

Export multiple device groups

Export the details of your device groups to a CSV file for record-keeping or bulk updates.

Use this task to create an export of all device groups in the system. You can modify the CSV file and import it again to update device group data.

Procedure

Step 1 From the main menu, choose **Device Management** > **Device Groups**.

Step 2 Click the export icon to download the device group details in CSV format.

The CSV file containing all device groups is downloaded in your systems download folder.

Device details available from the topology map

The topology map displays comprehensive information about network devices, including:

- Device specifications,
- Routing configurations, and
- Device links

You can use the topology map to monitor and manage your network devices efficiently.

For information on managing your devices and inventory, viewing interface details, and performing actions such as inventory synchronization, refer to the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management* guide.

View basic device details

View essential information about a networking device and its connectivity in a graphical topology map.

Use this task when you need to identify device details such as host name, status, IP address, and type within the topology view. The topology map allows you to visually explore device connections and adjust your view as needed. If you are viewing the HTML version of this guide, click on the images to view them in full-size.

Note Starting from Crosswork Network Controller version 7.2, interface names are not discovered if any communication protocol on a device is in a degraded state, even if SNMP and SSH protocols are working. If one protocol such as Telnet fails, the device is marked as degraded, preventing interface discovery and causing the link icon to remain blue. Removing the failing protocol allows interface names to be discovered and the link icon to turn green. Interface names are then populated and links show green if SNMP and SSH are functional, despite other protocol failures.

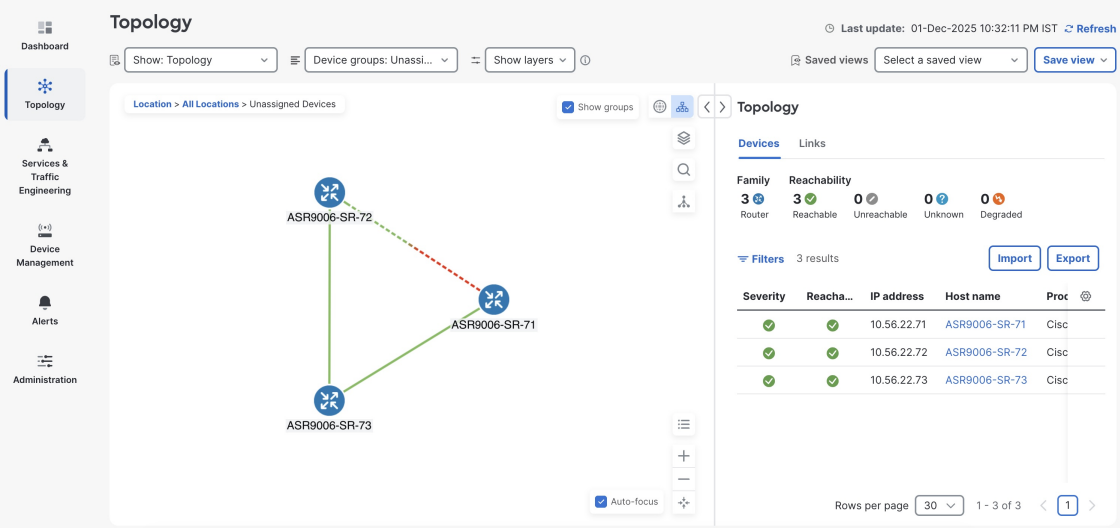
Procedure

Step 1 From the main menu, choose **Topology** .

Step 2 In the topology map, locate the device you want to inspect.

Step 3 Hover over the device icon, to quickly view the host name, reachability state, IP address and type of device.

Figure 70: Basic device details



Step 4 (Optional) Adjust the map view by zooming, panning, or rotating as needed for clarity.

You see basic device information, helping you quickly understand device status and network placement.

View all device details

Display comprehensive device information from the topology map, including its location, the type of device, and the date it was last updated.

Perform this task when you need to assess or troubleshoot a device directly from the topology view.

Before you begin

(Optional) Element Management Functions must be installed to view extended device details.

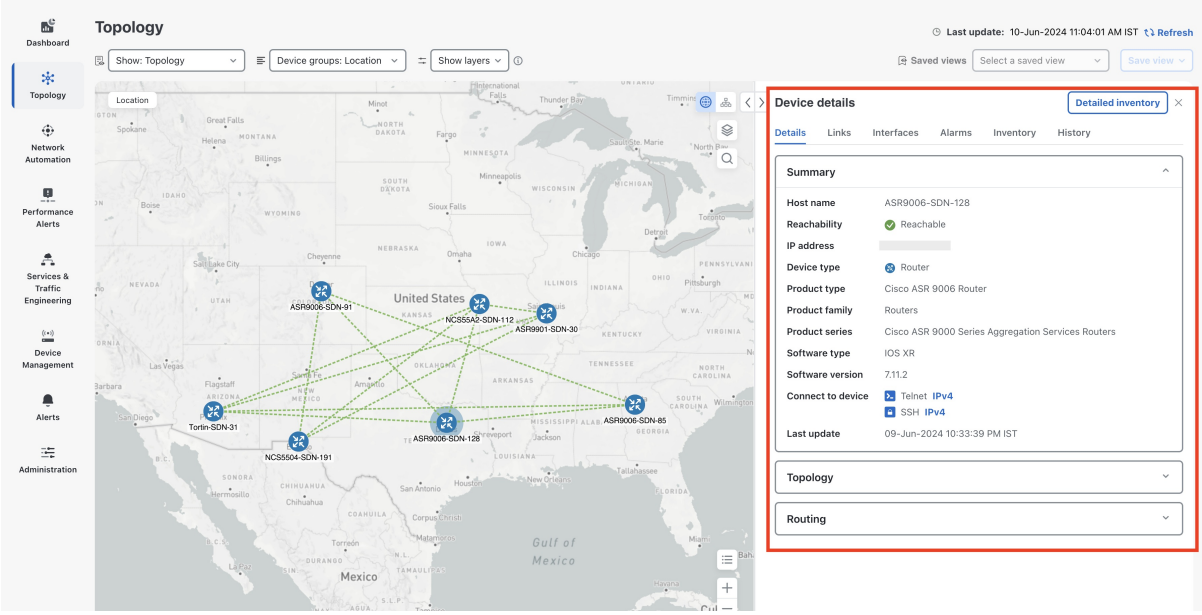
Follow these steps to view device details:

Procedure

Step 1 From the main menu choose **Topology** .

Step 2 Click the device icon that represents the device you want to inspect. The device detail window displays these tabs.

Figure 71: Device details



If you have installed Element Management Functions, the additional information is displayed in the **Device details** screen.

- Alarm information under Summary in the **Details** tab.
- An **Interfaces** tab with name, and operational and admin status for each associated interface.
- A **Links** tab with the details of the links on the selected device.
- An **Alarms** tab displaying information such as severity, source, category, and condition of the alarms. The columns can be customized based on your preferences.
- An **Inventory** tab displaying the product name, product ID, admin status, operational status, and serial number. The columns can be customized based on your preferences.
- A **History** tab with detailed information about device performance, including various performance metrics for CPU utilization, device memory utilization, device availability and environmental temperature. For each trend, you can choose the required time frame and dates using the Zoom and Date options on the graph. You also have the option to download the details in a PNG or CSV file.

The **Device details** panel provides all available information about the selected device. Additional details are shown if Element Management Functions are installed.

View the detailed device inventory

Provide an up-to-date and comprehensive view of each device's hardware components and attributes.

Use this task to quickly examine modules, chassis, cards, and interfaces for any device in your network, supporting maintenance, troubleshooting, and audits.

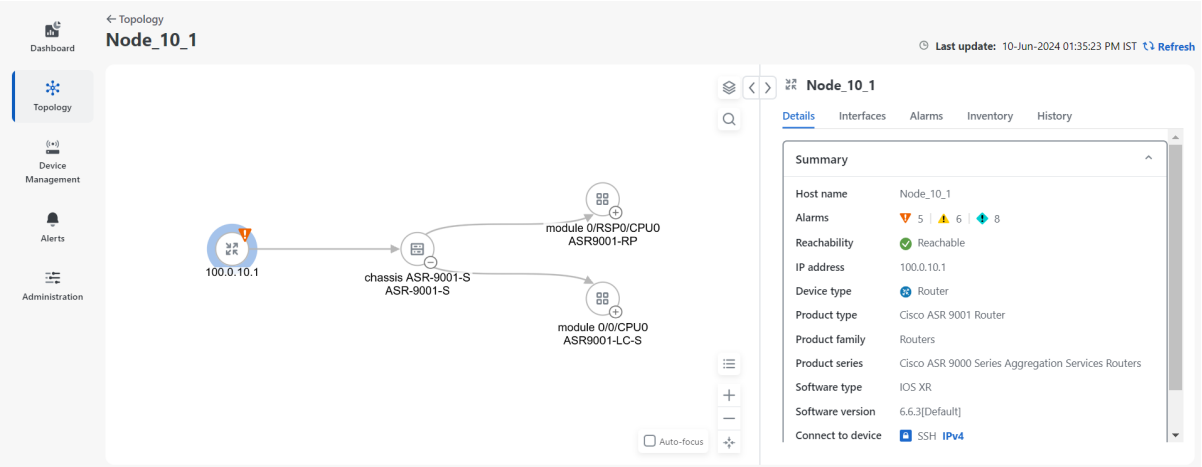
Before you begin

Procedure

Step 1 From the main menu, choose **Topology** .

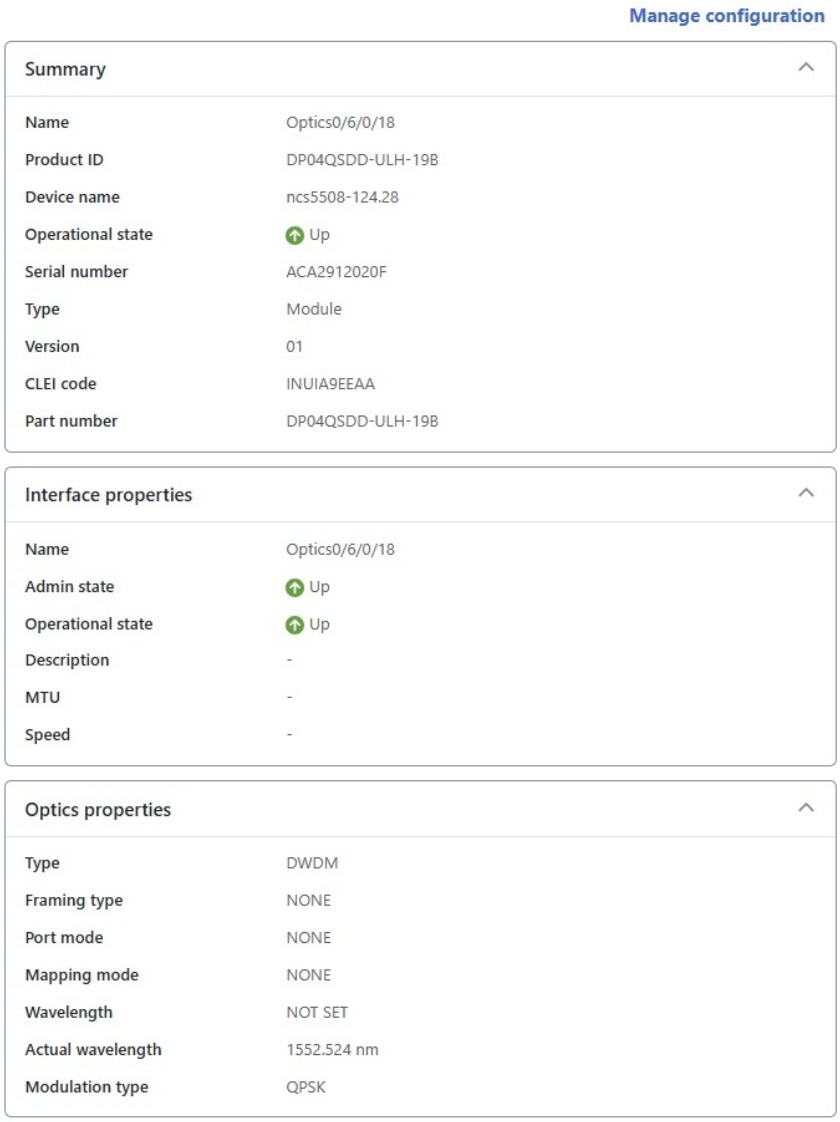
Step 2 Click the device icon to view the **Device details** pane for the device.

Step 3 Click the **Detailed inventory** button on the **Device details** pane to open the detailed inventory window for the chosen device. You can see the Topology tree view on the left.

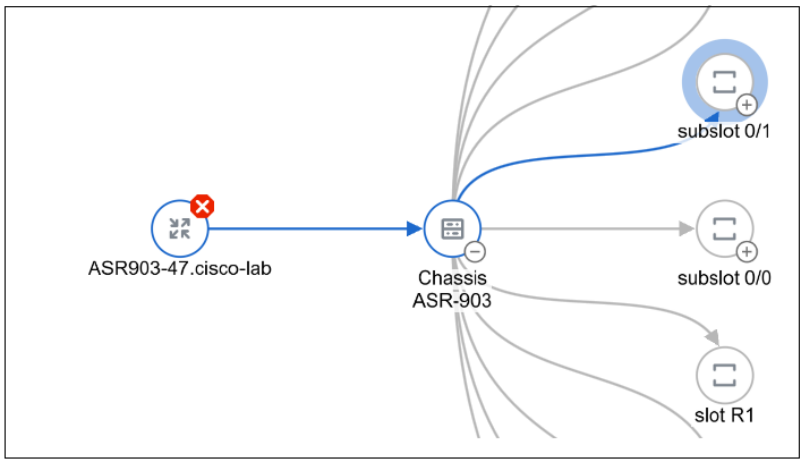


Under the **Details** tab, you can view detailed device information, including the device summary and interface properties.

Figure 72: Extended view of the Details tab



Step 4 Zoom in to view the different modules and click one for which you need detailed information.



You can view detailed information in the **Details, Interface, Alarms, Inventory and History** tabs for the chosen module.

Note
In the **Detailed inventory** view:

- Slot, bay, and container are not shown.
- The Optics Controller and pluggable components are combined and displayed as a single merged port.
- Only entities with the serial numbers (SN) are shown. An entity without a SN is hidden, and its child is attached to the parent of the hidden entity.
- Optical ports for XR devices are merged with the corresponding SFP and the RSIP. Ethernet port merging for XR devices is not supported.
- When you select the device or chassis node in the topology tree, both physical and logical interfaces are shown. Other nodes show only physical interfaces.

You can view detailed inventory attributes for any device, including modules, summary, interface properties, alarms, and history, supporting informed operations and troubleshooting.

Identify the device routing details

Find out how data packets are routed through a specific device in your network topology.

Use this task to view path configuration, or review routing details for devices within the topology map.

Before you begin

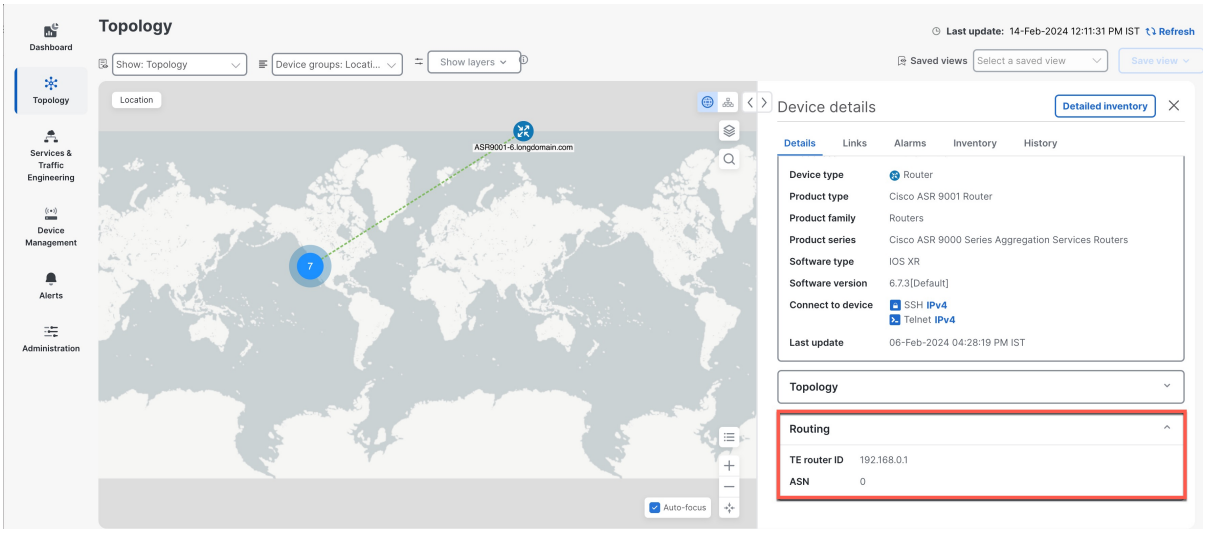
Follow these steps to identify the device routing details:

Procedure

Step 1 From the main menu, choose **Topology**.

Step 2 Click the icon for the device you want to view on the topology map.

The routing details for that device are displayed in the right pane.



You can view routing information for the selected device, including network paths and connections.

View links on a device

Display all network links currently connected to a device.

Use this task to quickly see which other network devices are connected to a specific device through direct links.

Before you begin

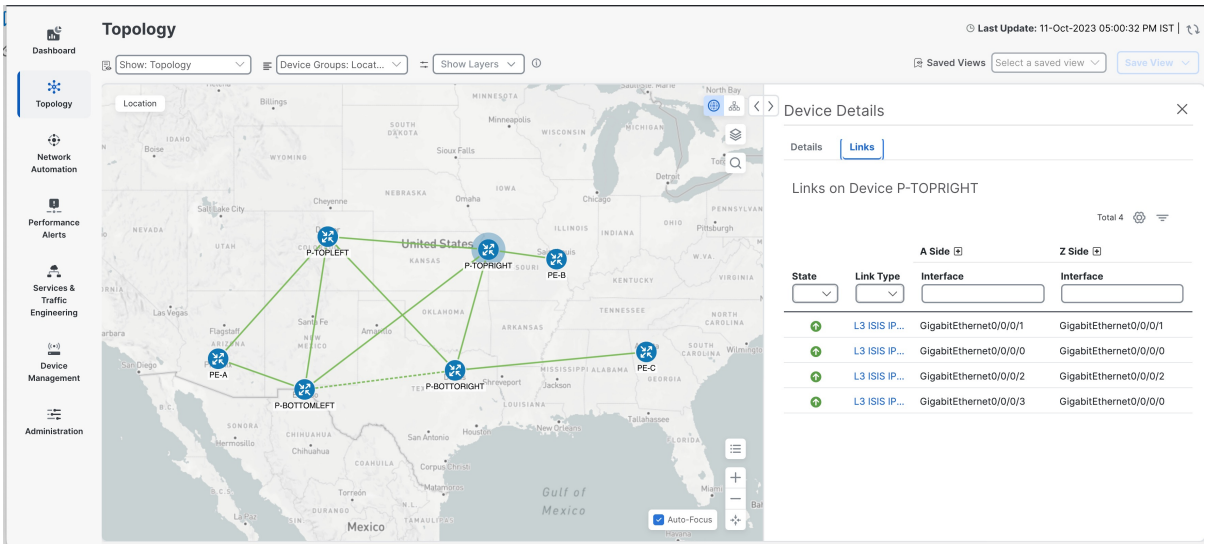
Make sure the device you want to view is already discovered and listed in the topology.

Procedure

Step 1 From the main menu choose **Topology**.

Step 2 Select the device icon for the device you want to inspect.

Step 3 In the **Device details** panel, click the **Links** tab.



You can see detailed information about every link connected to the device, including link state and associated neighbor devices.

Topology links

A topology link is a network mapping element that

- connects two devices within the network topology,
- reports key properties such as link name, source and destination devices, status, bandwidth, and latency, and
- provides real-time metrics, including utilization, traffic volume, and packet drops.

SR-PM delay and jitter metric availability

Delay and jitter metrics are available only when Segment Routing Performance Monitoring (SR-PM) is enabled. This comes with the Crosswork Network Controller Advantage package. For details on enabling SR-PM for links, refer to the *Enable SR-PM Monitoring for Links and TE Policies* section in the Cisco Crosswork Network Controller 7.2 Service Health Monitoring guide.

View the link details

View comprehensive link details, including link name, state, type, endpoint interface, and aggregation within the topology. Refer the **History** tab that provides useful insights into the performance and trends of the network. You can select the time interval to analyze the data.

You can view the link details for each link. For more information on the link state, refer to Link states and discovery methods, on page 338

Before you begin

LAG (Link Aggregation Group) discovery must be enabled to view LAG bundle members.

Procedure

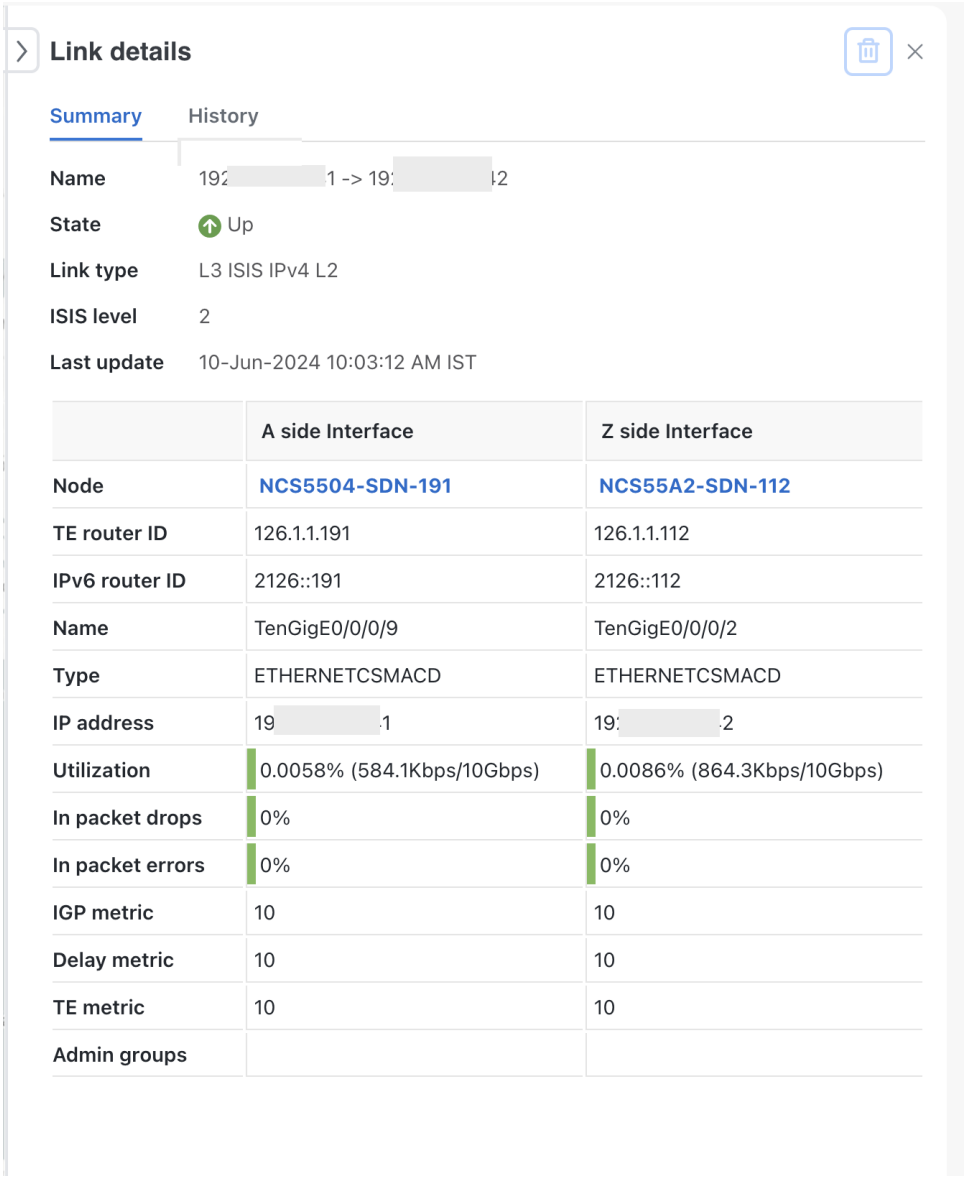
Step 1 From the main menu, choose **Topology** .

Step 2 Select a link to view details. You can:

- Click a link directly on the topology map.
- In the **Links** tab within the topology map, click a specific link.
- In the **Links** tab on the **Device details** page, click a specific link.

The link details pane displays link name, state, type, endpoint interfaces, and available history.

Figure 73: Link details



Step 3 Click a dashed line in the topology map to view aggregate link details.

A dashed line represents an aggregated link that includes multiple physical links.

Step 4 Review the interface details in the link details pane to view IPv4 unnumbered interface information, if available.

IPv4 unnumbered interfaces information is displayed as a combination of the TE Router ID and the index.

Crosswork Network Controller displays detailed link information as you select each link, including link state, type, endpoints, aggregation, link history, and LAG member data if available.

What to do next

If you enabled LAG discovery, allow a few minutes for data collection to complete.

View link interface metrics

Access and interpret key performance indicators for a network link to assess communication quality and troubleshoot issues.

Review link interface metrics to monitor bandwidth, delay, jitter, and packet loss on communication links between network devices. These insights help optimize resources and plan for network upgrades.

Before you begin

Procedure

Step 1 From the main menu, choose **Topology**.

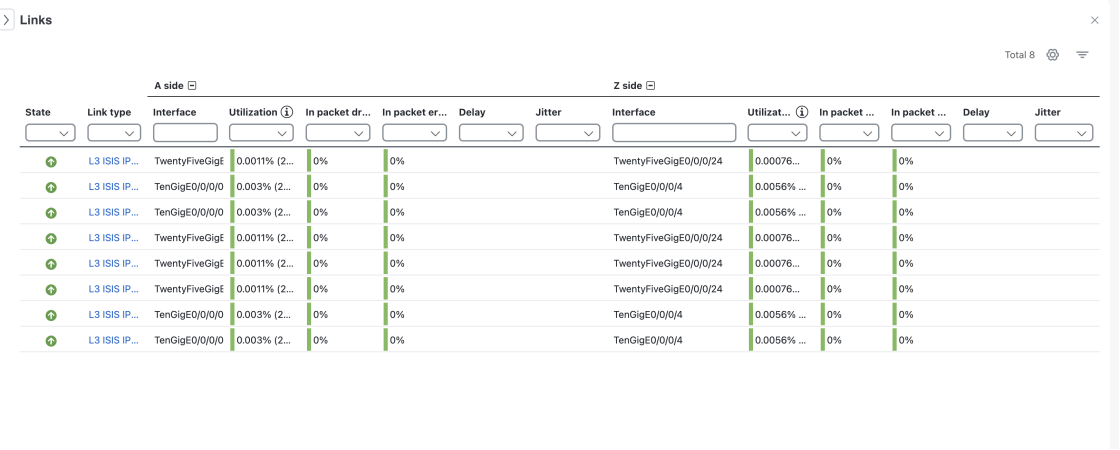
Step 2 Click a link on the topology map.

Step 3 Expand either **A side** or **Z side** to display interface metrics.

The utilization for IPv4 and IPv6 links shows total traffic and packet drops for the interface as a whole, not separately by address family. Combined values are reported for traffic metrics.

Metrics may include bandwidth, delay, jitter, and packet loss.

Figure 74: Link Interface Metrics



You can review comprehensive interface metrics to monitor link performance.

Link states and discovery methods

A link state and discovery method are network routing concepts that

- enable routers to maintain an up-to-date map of the network topology,

- allow routers to recognize and identify their neighbors using communication techniques such as static configuration, broadcast, multicast, or unicast, and
- determine the operational status of network links (such as up, down, or degraded) to optimize routing decisions.

Link types, discovery and states

The table summarizes typical link types, discovery methods, and how link states are determined:

Table 43: Link Types, Discovery and States

Link type	Discovery method	Link state
L3 link (ISIS, OSPF and eBGP)	via SR-PCE	• SR-PCE set it to UP or DOWN based on the link operational state • When one direction of a link is operational while the other direction is down, then the link state is set as degraded.
L2 link (CDP, LLDP, LAG)	via SNMP MIB: CDP, LLDP and LAG	The link state is based on the two link endpoints operational states (via IF MIB). • Link state is UP when initially discovered. • When one of the endpoint interfaces is operationally down, then the link state is set to DOWN. • When both endpoint interfaces are operationally up, then the link state is set to UP. • When one direction of a link is operational while the other direction is down, then the link state is set as degraded.

IF-MIB data collection

Starting with the 7.2 release, `IF-MIB`, interface-related inventory required for link discovery is collected through the Crosswork Network Controller inventory framework. Refer Crosswork Network Controller APIs to manage interface types for links discovery.

For details about interface inventory behavior and updates, see the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management Guide*.

Protocols for topology services

The table outlines the protocols and methods utilized to provide topology information, their key attributes, and typical use cases

Protocol/Method	Provides	Use Cases
IGP/ BGP-LS (via SR-PCE)	Real time topology including nodes, links, link metrics and similar attributes	L3 topology visualization
PCEP (via SR-PCE)	Real time LSP status and CRUD of SR-PCE initiated LSPs	• SR/SRv6, RSVP-TE LSP visualization • SR-PCE initiated LSP create/update/delete actions
SNMP (SNMPv2-MIB, IP-MIB, IF-MIB, LLDP-MIB, (CISCO CDP-MIB) (via CDG)	System info,rmation, interface table (interface and SR-TE/RSVP-TE traffic Utilization) IP address tables and L2 adjacency information	Supports device management, provides device details, and enables model building for Crosswork Optimization Engine. • L2/L3 topology • Interface name, admin/oper status • Interface and SR policy and RSVP-TE tunnel utilization
CLI (via CDG) - show mpls	TE router ID and so on.	Used to match the DLM node with the same TE router ID that is learned from the SR-PCE

Change L2 discovery settings

Control whether L2 (Layer 2) topology links using LLDP, CDP, and LAG protocols are visible on network maps.

L2 discovery allows the system to detect neighboring devices and their connections using LLDP, CDP, and LAG protocols. By default, this feature is disabled. When disabled, these topology links (including ones previously discovered) are hidden from maps. Enabling discovery makes protocol-based links visible.

Before you begin

Ensure all pods are healthy before changing L2 discovery settings.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings**.

Step 2 Under **Topology**, click the **Discovery** option.

Step 3 Select or clear the checkboxes for the protocols you want to enable or disable.

Step 4 Click **Save**.

The visibility of L2 topology links updates on network maps according to the protocols you selected.

What to do next

When you enable discovery, the system automatically creates the required collection jobs. For details about each collection job, see L2 discovery protocol collection jobs, on page 341.

L2 discovery protocol collection jobs

When discovery is enabled, Crosswork Network Controller creates the required collection jobs for each L2 protocol. The table describes, for each supported protocol setting, the collection job IDs, context IDs, MIBs collected, and relevant sensor paths.

Table 44: Collection Jobs for each setting

L2 Configuration Setting	Helios collection Jobs ID	Context ID	MIBs collected	Sensor paths
None (default)	cw.topo_svc	`cw.toposvc.snmp` `cw.toposvc.snmptraps`	`IF-MIB, IP-MIB, LAG-MIB` IF-MIB:notification **Note** Starting with the 7.2 release, `IF-MIB` data is collected using interface-related inventory through the Crosswork Network Controller inventory framework. Refer Crosswork Network Controller APIs to manage interface types for links discovery. For details about interface inventory behavior and updates, see the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management Guide*.	`IP - MIB : IP-MIB / ipAddressTable / ipAddressEntry` `IF-MIB:notifications`

L2 Configuration Setting	Helios collection Jobs ID	Context ID	MIBs collected	Sensor paths
CDP	cw.topo_svc	cw.toposvc.cdp	IF-MIB, CDP-MIB, LAG-MIB	CISCO - CDP - MIB : CISCO - CDP - MIB / cdpCacheTable / cdpCacheEntry CISCO - CDP - MIB : CISCO - CDP - MIB / cdpInterfaceTable / cdpInterfaceEntry
LLDP	cw.topo_svc	cw.toposvc.lldp	IF-MIB, LLDP-MIB, LAG-MIB	LLDP - MIB : LLDP - MIB / lldpLocPortTable / lldpLocPortEntry LLDP - MIB : LLDP - MIB / lldpRemTable / lldpRemEntry
LAG	cw.topo_svc	cw.toposvc.lag	IF-MIB, LAG-MIB	IEEE8023 - LAG - MIB : IEEE8023 - LAG - MIB / dot3adAggTable / dot3adAggEntry IEEE8023 - LAG - MIB : IEEE8023 - LAG - MIB / dot3adAggPortTable / dot3adAggPortEntry

Common errors for topology discovery settings

The table lists common errors that occur when enabling or disabling topology discovery, along with recommended actions to resolve each issue.

Table 45: Common error scenarios

Possible error scenario	Cause	Recommended action
After disabling, some of the disabled links are displayed in the maps.	A protocol that is disabled soon after being enabled may cause a problem. The system may stop the collection job for the previous enabled job before it finishes processing the SNMP data. This may lead to a mismatch between the actual and the displayed status of the links. The links that are disabled may still appear as enabled.	Enable and disable the protocol again with sufficient wait time in between, or restart robot-topo-svc. To restart the robot-topo-svc, refer to Monitor Platform Infrastructure and Application Health.
When you try to enable discovery, the helios job fails and settings are disabled from further editing.	A possible cause of the collection job being stuck in an unsuccessful state is that the helios pod is unhealthy. Crosswork prevents users from modifying the L2 discovery settings while the collection job is in progress. This means that the collection job cannot be canceled or restarted until the helios pod is healthy again.	Ensure that the pods are healthy, and then enable and disable the protocol with sufficient wait time in between,or restart robot-topo-svc. To restart the robot-topo-svc, refer to Monitor Platform Infrastructure and Application Health.
When you change the discovery settings, the topology UI or topology service crashes resulting in an unpredictable status.	The mechanism to disable users from further editing while the collection job is being created or deleted, relies on pods communicating via Postgres flag. If any pod crashes during this time, the Postgres flag key is not set correctly.	

Import a KML file

Add devices and their geographic locations to the topology map by importing a formatted Keynote Markup Language (KML) file.

Use this task when you want to visually map devices on a topology map according to their location information contained in a KML file.

Before you begin

If you do not have a device KML file:

- Download the KML file template.
- Open the template using your preferred tool.
- Add one row for each device with the necessary information.

- Save the updated KML file.

Procedure

Step 1 From the main menu, choose **Topology**.

Step 2 Click to open the **Import KML File** dialog box.

Step 3 Click **Browse**, select your KML file, and click **Open**.

Step 4 With the KML file selected, click **Import**.

Caution
Wait for the operation to finish before clicking **Import** again to avoid duplicate entries.

Devices and their locations appear on the topology map.

Export geographical data to a KML file

Obtain a KML file containing location information for network devices, which can be reused or imported into external mapping tools.

Use this task when you want to back up, share, or analyze device locations outside the current application.

Procedure

Step 1 From the main menu, choose **Topology**.

Step 2 In the right pane, click **Export KML file**.

The KML file containing device location data is downloaded to your system's default download folder.

Customize your topology map display

Enable visibility and personalize display options for devices, links, and alarms on your topology map to suit operational needs.

Use this task when you want to highlight specific device states, link characteristics, or alarms for network monitoring.

Before you begin

Procedure

Step 1 From the main menu, click **Topology**.

Step 2 On the topology map, open the **Display preferences** dialog box.

Step 3 In the **Devices** tab:

a) Show or hide device state.

b) Select your preferred label type, such as host name, IP address, or OSPF Router ID.

Step 4 In the **Links** tab:

a) Toggle the option to distinguish aggregated links from single links.

Note
Aggregated dual stack links are displayed as a single line.

b) Choose the link color scheme based on down state or utilization. If you select utilization, set the appropriate thresholds.

Step 5 In the **Alarms** tab:

a) Show or hide device-level alarms.

b) Filter alarms by severity to display only those at or above your chosen threshold.

The topology map updates to reflect your selected device, link, and alarm display preferences, providing a tailored view for effective network monitoring.

Assign colours to link health thresholds

Configure colour thresholds for link health to enhance real-time monitoring and visualization of the network status

Link health is visualized in both logical and geographical maps. Assigning colour thresholds to metrics helps you quickly identify potential issues in network links.

Before you begin

- Verify that Segment Routing Performance Monitoring (SR-PM) is enabled if you want to use delay and jitter metrics. Enabling SR-PM requires installation of Service Health, available as part of the Crosswork Network Controller Advantage package.
- Refer to the *Enable SR-PM monitoring for links and TE policies* section in the *Cisco Crosswork Network Controller Service Health Monitoring guide* for detailed steps.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings**.

Step 2 Under **Topology**, select **Metric thresholds**.

Step 3 Define the colour criteria for links. Each row defines a color and the percentage range that the color will represent.

- For each row, specify a colour and the percentage range it represents.
- Enter values in the **To** fields only, each row starts from the end of the previous row's range.
- Ensure that ranges are sequential, with no overlaps. For example, after a 0-25% range, the next row must begin above 25%.
- Assign a unique colour to each threshold. Do not reuse colours for multiple ranges.
- Colour-coded link thresholds apply to metrics such as bandwidth utilization, delay, jitter, packet errors, and packet drops.
- Delay and jitter metrics are only available when SR-PM is enabled.

The topology map updates to reflect your colour threshold settings and device state preferences, improving visibility into network health.

Troubleshooting the topology map

The table below lists common topology map issues, their possible causes, and suggested actions:

Issue	Possible cause	Recommended action
Devices do not appear on the topology map	Devices are offline or unreachable	Verify devices are powered on and connected to the network.
Incorrect topology layout	Outdated network configuration	Ensure device IP addresses, subnet masks, gateways, and DNS settings are correct.
Status shows as "unknown" or "unreachable"	Network or configuration error	Check device connectivity and management protocol settings.
Map does not match physical layout	Devices added or removed without update	Refresh the topology map after any network changes.

If the basic troubleshooting steps do not resolve your topology issue, refer these actions for further diagnosis.

- Search for missing Layer 2 links that could cause connectivity gaps.
- Search for missing Layer 3 links that could impact routing.
- Check for error records in the Alarm and Events report in Topology Services for additional details.
- Rebuild the topology to refresh the network structure.

Find missing Layer 2 links

Identify and correct issues that prevent Layer 2 links from appearing in the topology. For more information refer to Change L2 discovery settings, on page 340.

Missing Layer 2 links typically occur if L2 discovery protocols are not enabled or required device and peer configurations are incomplete. Ensuring proper discovery settings and connectivity allows accurate network topology visualization.

Procedure

Step 1 From the main menu, go to **Administration** > **Settings** > **System settings**.

Step 2 Under **Topology**, select **Discovery**.

Step 3 Enable L2 link discovery if it is disabled, then click **Save**.

Step 4 If L2 links are still not visible, perform the following checks:

a. Check PCE configuration:

- Ensure the required PCE IP address is assigned to a loopback interface.

```
pce
 address ipv4 198.19.1.201
```

- Configure the API user required for discovery.

```
api
 user cisco
  password encrypted 121A0C041104
```

- Configure any required sibling PCE addresses and verify they are visible.

```
sibling ipv4 11.1.201.202
```

b. Verify sibling PCE connectivity:

```
RP/0/RP0/CPU0:pce-1#show pce api sibling connection
```

Sample output:

```
Address:                   11.1.201.202
Connected:                        Yes
Input buffer size:                  0
Packets in output buffer:           0
```

c. Ensure the head-end node is a PCEP peer and correctly configured:

```
segment-routing
 traffic-eng
  pcc
   source-address ipv4 198.19.1.4
   pce address ipv4 198.19.1.201
   precedence 100
   pce address ipv4 198.19.1.202
   precedence 100
   report-all
```

d. Verify PCEP sessions:

- On PCE

```
RP/0/RP0/CPU0:pce-1#show pce ipv4 peer 198.19.1.4
```

- On PCC

```
Node-4#show segment-routing traffic-eng pcc ipv4 pee
```

Sample output:

```
Peer address: 198.19.1.201,
  Precedence: 100, (best PCE)
```

```
    State up
    Capabilities: Stateful, Update, Segment-Routing, Instantiation, SRv6

  Peer address: 198.19.1.202,
    Precedence: 100
    State up
    Capabilities: Stateful, Update, Segment-Routing, Instantiation, SRv6
```

Step 5 If L2 links still do not appear, consider rebuilding your topology. For details, see Rebuild the topology.

After completing these steps, missing Layer 2 links should be discovered and visible in the network topology view. If issues persist, rebuilding the topology may resolve configuration inconsistencies.

What to do next

Review newly discovered L2 links and confirm connectivity in the topology.

Find missing Layer 3 links

Identify and restore missing Layer 3 links by checking device health, configurations, and SR-PCE topology information.

Missing Layer 3 links can occur due to device-level issues such as hardware failure, software bugs, misconfiguration, or interference. Ensuring that devices and IGP settings are correct helps the SR-PCE learn accurate topology information.

Before you begin

Procedure

Step 1 From the main menu, go to **Administration** > **Manage Provider Access**.

Under **Reachability** column, confirm that the providers are reachable.

Step 2 If the L3 links are not visible:

a) If a link is missing in the topology UI, ensure that the ISIS or OSPF neighbor relationship is up using these configurations:

```
RP/0/RP0/CPU0:Node-4#show isis neighbors
```

Sample output:

```
IS-IS 1 neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
Node-7         Gi0/0/0/0        *PtoP*         Up    23       L2   Capable

RP/0/RP0/CPU0:Node-7#show isis neighbors
```

Sample output:

```
IS-IS 1 neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
Node-4         Gi0/0/0/1        *PtoP*         Up    22       L2   Capable
```

b) Ensure that the link is configured as point-to-point:

```
router isis 1
interface GigabitEthernet0/0/0/0
  point-to-point
```

c) Ensure that the link is visible in PCE:

```
show pce ipv4 topology 198.19.1.4
```

Sample output:

```
Node 30
  Link[2]: local address 10.4.7.4, remote address 10.4.7.7
```

d) In case the L3 links are still missing, consider rebuilding your topology. Refer to Rebuild the topology.

Check error records in Topology services alarms and events report

Diagnose and resolve problems within Topology services by reviewing error records in the Alarm and Events report.

Topology services may encounter operational errors, such as missing data, communication failures, or configuration issues. These errors are captured in the Alarm and Events report, allowing you to quickly identify and address problems impacting network visibility.

Procedure

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

Step 2 In the Source filter, enter `topo` to display alarms and events specific to Topology services.

The filtered Alarm Events report shows all related error records.

Step 3 Review the list for error records, noting any issues such as missing data or communication failures.
You will see all error records associated with Topology services, making it easier to diagnose and resolve operational problems.

What to do next

Investigate any error records found and take corrective actions as needed.

Rebuild the topology

Rebuilding the topology is a process of creating a new topology for our system. This is useful when the topology becomes inconsistent because of network problems or other unforeseen events. You should only rebuild the topology as a last resort.

The topology rebuild will refresh the topology and update the links and devices. The topology pages will not display links and devices when a rebuild is in progress. They will reappear after the rebuild is complete.

Procedure

Step 1 Turn the system maintenance mode on.

Choose **Administration** > **Settings** > **System Settings** > **Maintenance mode**.

Step 2 Begin the process of rebuilding the topology.

Under **Topology**, choose **Maintenance** and click **Rebuild Topology**.

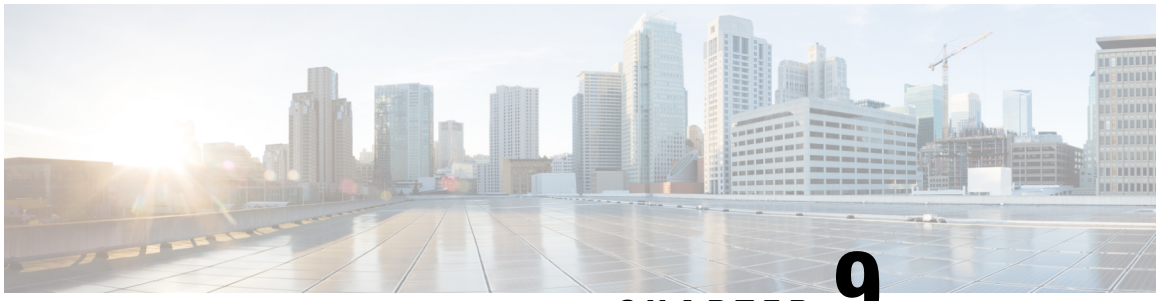
Step 3 When the **Confirm Topology Rebuild** dialog box appears, click **Rebuild Topology** again.

Step 4 After links and devices reappear on the topology map indicating that the topology has been rebuilt, turn the maintenance mode off.

Choose **Administration** > **Settings** > **System Settings** > **Maintenance mode**.

Step 5 (Optional)You can view detailed events about the rebuild.

a) Choose **Alerts** > **Alarm and Events**.
b) From the **Show** drop-down list, select **Events**.
c) From the **Category** drop-down list, select **Network**.



CHAPTER 9

Manage and Customize Dashboards

This chapter shows how to create, edit, delete, and customize dashboards so you can quickly view and manage the information you need.

Dashboards and dashlets

A dashboard is a centralized interface that displays the summary of metrics and trends through interactive components called dashlets. Dashboards appear as individual tabs, allowing you to monitor and compare different sets of data in a single view.

Dashboard helps you monitor and analyze performance across various policies by highlighting the most relevant metrics. Crosswork Network Controller provides a set of default dashboards, which you can personalize by adding or customizing additional dashlets to meet your specific monitoring needs.

The data displayed in each dashlet is polled based on the configured policies. Some dashlets allow you to edit the metrics to customize the displayed data. For information on the policies, see the *Monitor device and inventory health* chapter in the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management* guide.

Dashboard customizations

The dashboard framework includes the customization options to help you tailor dashboards to your specific needs:

- Multiple dashboard tabs per user: Create and manage several dashboards to monitor different data views or operational areas.
- Dashboard actions: Add, copy, rename, or delete dashboards as needed to stay organized and focused on your goals.
- Dashlet actions: Add, edit, copy, and delete dashlets to control how information is displayed and shared.
- Dashboard-level filters: Apply filters across the entire dashboard to view the device group or port-based data.
- Save and load views: Capture customized dashboard layouts and reload them as needed, so you can quickly switch between different monitoring scenarios.

These capabilities make it easy to create a flexible, data-driven workspace that evolves with your business needs.

Customization of dashboards

Dashboards in Crosswork Network Controller provide a centralized, customizable view of key metrics through interactive dashlets.

Use these topics to create, customize, and manage dashboards:

Create a dashboard

You can create multiple dashboards. Each dashboard is represented as a separate tab. The Crosswork Network Controller includes a default dashboard tab named General, which you cannot rename, delete, or apply filters.

To create a custom dashboard and add relevant dashlets, perform these steps:

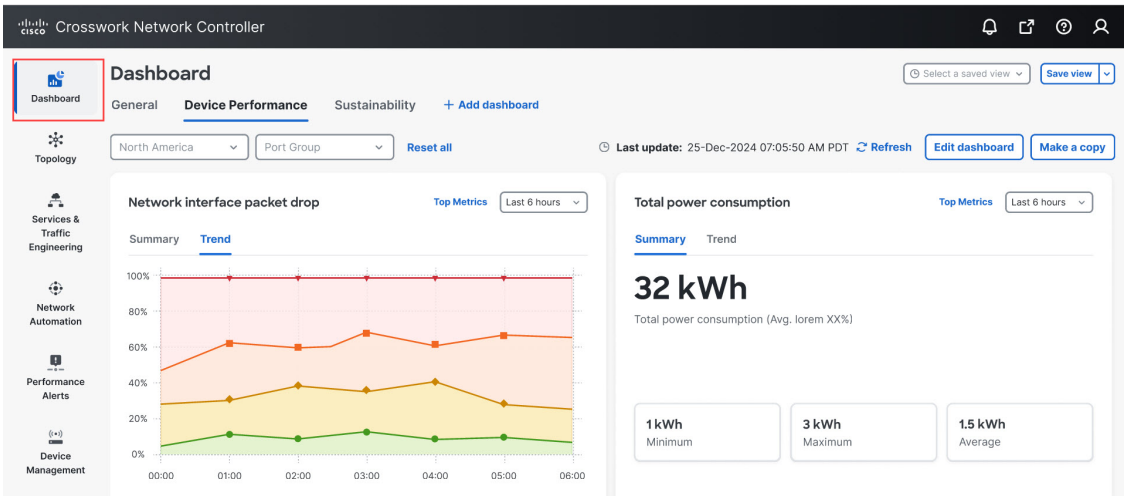
Before you begin

Ensure that you have configured the policies that you want to monitor. For information on the policies, see the *Monitor device and inventory health* chapter in *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management* .

Procedure

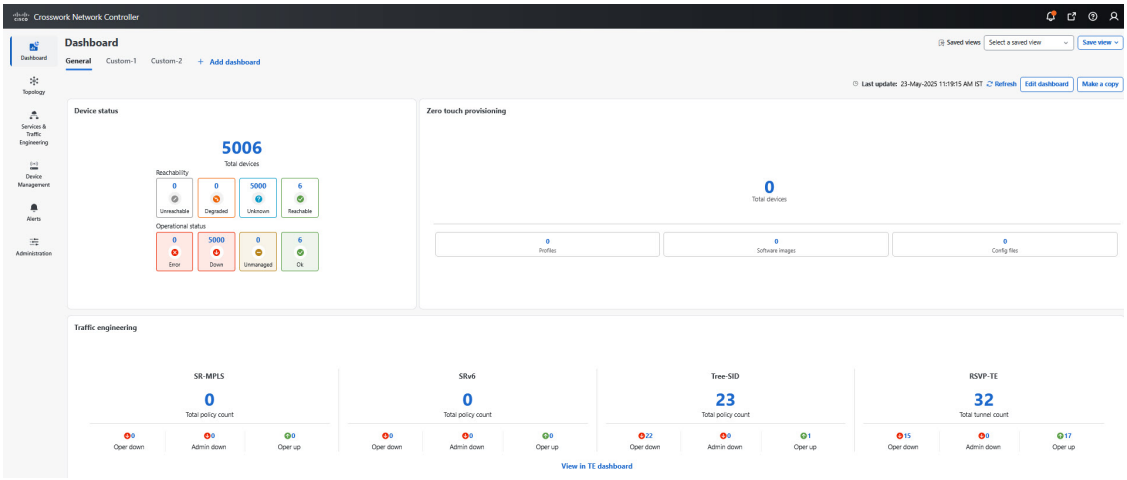
Step 1 From the Crosswork Controller Network main menu, navigate to **Dashboard** .

Figure 75: Dashboard



The **Dashboard** page opens with the default **General** tab.

Figure 76: Dashboard - General tab



Step 2 Click **+ Add Dashboard** to create a new dashboard tab.

Step 3 Click the edit icon next to the default title, and enter a meaningful name for the dashboard.

Step 4 Add dashlets:

a) Click **+Add dashlet** .

b) In the **Add Dashlets** drawer, select the policy and the corresponding metrics you want to monitor.

Note
If you choose to add the Top 5 metrics in the **Interface health** dashlets, you must create an Interface health monitoring policy by using either device groups or port groups. You can create one or multiple of these groups. If you configure the Interface health policy using individual devices, rather than device or port groups, the data will not appear in the **Dashboards**. However, the data will still be accessible on the **Device Management > Top Metrics** UI page.

c) Click **+Add** .
The selected dashlets are added to the dashboard.

d) Enter a unique, meaningful title for each dashlet.
e) Click the ellipsis icon (⋯) on a dashlet to:
    - configure the chart type as Bar, Donut, or Pie, and
    - copy or delete the dashlet.

Step 5 Click **Save** .

The selected dashlets appear on the dashboard.

What to do next

To view relevant data on the dashlets, apply the appropriate device or port group filters. Then, select the time range for which you want to view the data, such as 6 hours, 1 day, 1 month, and so on.

Edit a dashboard

You can modify a custom dashboard by renaming it, adding or removing dashlets, changing chart types, and editing the dashlet metrics.

To modify a dashboard and the relevant dashlets, perform these steps:

Before you begin

- Identify the dashboard tab you want to modify and confirm it is not the default dashboard, which cannot be edited.
- Review the existing dashlets to determine which elements such as titles, metrics, or chart types you want to update.

Procedure

Step 1 From the Crosswork Controller Network main menu, navigate to **Dashboard** .

The **Dashboard** page opens with the configured dashboards as individual tabs.

Step 2 Select the dashboard tab that you want to edit.

Step 3 Click **Edit dashboard** .

Step 4 Modify the required parameters:

- Dashboard title: Click the edit icon next to the dashboard title and enter a meaningful name.
- Dashlet title: Click the title field within a dashlet and enter a descriptive name.
- Chart type: Click the ellipsis icon (⋯) on a dashlet, select **Change chart type** , and choose from **Bar** , **Donut** , or **Pie** .
- Copy dashlet: Click the ellipsis icon (⋯) and select **Copy** . A duplicate dashlet appears after the last dashlet in the dashboard.
- Delete dashlet: Click the ellipsis icon (⋯) and select **Delete** to remove the dashlet from the dashboard.

- Modify metrics: Click **Edit metrics** to adjust or reset the metric range.

  Note
  This option is available only for certain dashlets, such as Link metrics.

Step 5 Click **Save** .

What to do next

-

Manage the dashboard views

You can save a dashboard view as a snapshot and reuse it to quickly access a specific configuration of dashlets, filters, and layout. You can share saved views with others or revisit them for common monitoring setups.

To manage the dashboard views, perform these steps:

Before you begin

If you want to rename or manage the existing views, verify that a view has been previously saved.

Procedure

Step 1 From the Crosswork Controller Network main menu, navigate to **Dashboard** .

The **Dashboard** page opens with the configured dashboards displayed as individual tabs.

Step 2 Select the dashboard tab for which you want to manage views.

Step 3 In the dashboard toolbar, click the views drop-down and perform any of these actions:

a) **Save view as** : Save the current dashboard layout and filters with a unique name.
b) **Rename view** : Update the name of an existing saved view.
c) **Manage views** : View and manage all saved views.

- Sort views by **Recently added** , **Most viewed**, or **Recently visited**.
- Delete any view that is no longer needed.

Filter data in a dashboard

You can filter the data visualizations in a dashboard using the drop-downs, which let you focus on the displayed metrics based on selected device groups or port groups.

Note

- You can filter data only in the custom dashboard. You cannot filter data in the General dashboard.
- You can apply only one filter at a time. For example, if you filter data using a device group, the dashboard displays results for that group. Later, if you filter by port group, it overrides the previous filter and displays data based only on the selected port group.

To filter data in a dashboard, perform these steps:

Procedure

Step 1 From the Crosswork Controller Network main menu, navigate to **Dashboard** .

The **Dashboard** page opens with the configured dashboards as individual tabs.

Step 2 Select the dashboard tab where you want to apply filters.

Step 3 In the dashboard view, use one of the relevant filter options:

- Device group: Click the **Device group** drop-down and select the desired group.
- Port group: Click the **Port group** drop-down and select the relevant port group.

Step 4 To sort data by time range, click the range drop-down and select a duration. For example, 6 hours, 1 day, 1 week, or 1 month.

Remove a dashlet

You can remove dashlets from a dashboard and add them again at any time.

To delete a dashlet from the custom dashboard, perform these steps:

Before you begin

Review the contents to confirm that no critical dashlets are in use.

Procedure

Step 1 From the Crosswork Controller Network main menu, navigate to **Dashboard** .

The **Dashboard** page opens with the configured dashboards as individual tabs.

Step 2 Select the dashboard tab from which you want to delete the dashlet.

Step 3 Click **Edit dashboard** .

Step 4 In the dashlet that you want to delete, click the ellipsis icon (⋯) and select **Delete** .
The dashlet is removed from the dashboard.

Step 5 When the confirmation message appears for the last dashlet, review the details carefully, then click **Delete** to permanently remove the dashlet.

Delete a dashboard

To delete a custom dashboard and the relevant dashlets, perform these steps:

Before you begin

- Document any important configurations or metrics before deleting.
- Review the dashboard contents to confirm that no critical dashlets or data views are in use.
- You cannot delete or modify the **General** dashboard. It contains system-generated dashlets related to the configured policies.

Procedure

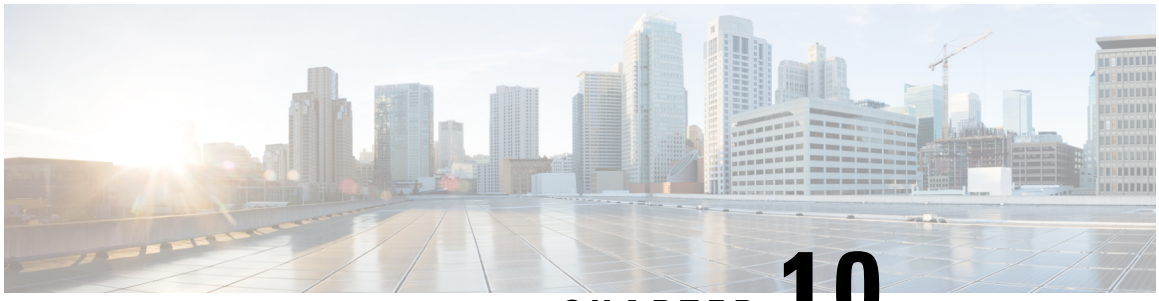
Step 1 From the Crosswork Controller Network main menu, navigate to **Dashboard** .

The **Dashboard** page opens with the configured dashboards as individual tabs.

Step 2 Select the dashboard tab that you want to delete.

Step 3 Click **Edit dashboard** .

Step 4 Click **Delete dashboard** .
When the confirmation message appears, review the details carefully. Click **Delete** to permanently remove the dashboard.



CHAPTER 10

Manage Licenses

This section contains the following topics:

Smart Licensing overview

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and your organization. It provides complete visibility into your software usage and gives you full control over your licensing status.

For detailed information on Cisco Licensing, go to cisco.com/go/licensingguide.

Benefits of Smart Licensing

These are the key benefits of Smart Licensing.

- **Easy activation**—Establishes a pool of software licenses that can be used across the entire organization—no more entering Product Activation Keys (PAKs).
- **Unified management**—Provides a complete view into all of your Cisco products and services in a user-friendly portal.
- **License flexibility**—Allows you to easily use and move licenses as needed since the software is not node-locked to your hardware.

Smart Licensing in Cisco Crosswork Network Controller

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com). A Cisco Smart Account is a repository for Smart enabled products and enables you to activate Cisco licenses, monitor license usage, and track Cisco purchases. All licenses you have purchased are kept in a centralized system called Cisco Smart Software Manager (CSSM), in customer specific Smart Accounts. With CSSM, you may create and manage multiple Virtual Accounts within your Smart Account to manage licenses. Cisco Crosswork Network Controller periodically sends the license usage information to CSSM. You can log in to your Smart Account to access the license utilization information.

Once the Smart Licensing service is active and you check out a license in the Cisco Crosswork Network Controller UI, the system enters the evaluation mode (up to 90 days) until the registration or reservation is completed. In evaluation mode, you will have access to all the features, but only for a limited duration of 90 days. After registration or reservation is completed, you can use all features until the license period expires. After the evaluation period of 90 days, if the product is still not registered with CSSM, or a reservation is not installed, all features will be marked as EvalExpired, and you will not be able to use any features until the smart license service is registered with CSSM or reservation is completed. Smart Licensing remains enabled, allowing you to register Cisco Crosswork Network Controller with CSSM or complete the reservation.

Note In a geo redundant setup, the Smart Licensing registration needs to be completed only on the primary active site. The license is consumed when geo redundancy is activated for the first time and will automatically sync with the standby site.

Lab system licenses

Licenses for lab systems are acquired through the same process as those for production environments. If you need a license for a lab beyond the 90-day trial period, please coordinate with your account team or a Cisco partner to obtain the appropriate license.

Smart Licensing workflow

These are the high-level steps involved in configuring Smart Licensing for Cisco Crosswork Network Controller:

1. Set up a Smart Account on Cisco Software Central. Go to Smart Account Request and follow the instructions on the website.
2. Configure the communication between Cisco Crosswork Network Controller and Cisco Smart Software Manager (CSSM). For details, see Configure transport settings, on page 361.
3. Register Cisco Crosswork Network Controller with CSSM. For details, see Register Cisco Crosswork Network Controller with CSSM using token, on page 361 and Register Cisco Crosswork Network Controller with CSSM using offline reservation, on page 363.

Configure transport settings

You can configure the transport settings to decide how Cisco Crosswork Network Controller communicates with CSSM.

Note You cannot modify the transport settings while the product is in the Registered state. You have to deregister to update them.

Follow these steps to configure the transport settings.

Procedure

Step 1 From the main menu, choose **Administration** > **Smart Licenses** to display the **Smart licenses** tab.

Step 2 The **Transport settings** field displays the current transport mode selected. To modify, click **View/Edit**. The **Transport Settings** dialog box appears.

Step 3 Select the relevant transport mode and enter the required information in the corresponding fields.

The available options include

- **Direct**—Cisco Crosswork Network Controller directly connects with CSSM.
- **On-prem Smart Software Manager**—Cisco Crosswork Network Controller communicates via CSSM On-Prem, ensuring that all user communication remains on premises. For details on the CSSM On-prem option, see the Smart Software Manager guide.
- **HTTP/HTTPS gateway**—Cisco Crosswork Network Controller communicates to the direct mode end point through an intermediate proxy server.

Step 4 Click **Save**.

Register Cisco Crosswork Network Controller with CSSM using token

To enable licensed features, the Cisco Crosswork Network Controller application must be registered to CSSM using a registration token. For information on generating a registration token, refer to the support resources provided in the Cisco Software Central web page. Once registered, an Identity Certificate is securely saved in the Smart Account and used for all ongoing communications. The certificate is valid for one year and will be renewed automatically after six months to ensure continuous operation.

Follow these steps to register Cisco Crosswork Network Controller with CSSM using token.

Before you begin

Ensure that you have a Smart Account. If not, go to Smart Account Request and follow the instructions on the website.

Procedure

Step 1 From the main menu, choose **Administration** > **Smart Licenses** to display the **Smart licenses** tab. The registration status and license authorization status displays **Unregistered** and **Evaluation mode** respectively.

Step 2 In the Smart Software Licensing information box at the top, click **Register**.

The Smart Software Licensing Product Registration dialog box appears. The **Register via token** radio button is selected by default.

Step 3 In the **Product instance registration token** field, enter the registration token generated from your Smart Account. Ensure that the token ID is accurate and within validity period.

Step 4 If you are re-registering the application, check the **Re-register this product registration if it is already registered** check box.

After a backup restore, disaster recovery, or data migration operation, you must manually re-register the Cisco Crosswork Network Controller with CSSM. This requirement applies if the Cisco Crosswork Network Controller VM was already registered at the time the backup was taken and is used in the restore operations.

Step 5 Click **Register**. It may take a few minutes to process the registration. If successful, the 'Product Registration completed successfully' message appears.

The registration status and license authorization status displays **Registered** and **Authorized** respectively.

Note

- It will take at least 20 seconds for the request to succeed. If you do not receive a correct response within the first 20 seconds, the system will continue to check every 10 seconds for up to five minutes. If no response is obtained after five minutes, the system will display a generic error message.
- If you encounter a registration error, for example, "Communication send error" or "Invalid response from licensing cloud", wait for some time and retry the registration. If the error persists after multiple attempts, contact the Cisco Customer Experience team.
- If you encounter a communication timeout error during registration, click **OK** in the error dialog box, and the application will reattempt the registration.
- In some cases, after successful registration, the page may need to be refreshed manually to see the updated status.

Perform licensing actions manually

The renewal of registration and authorization is automatically enabled in Cisco Crosswork Network Controller, by default. However, when the communication fails between the application and CSSM, you can manually initiate these actions.

Follow these steps to manually renew, re-register, or deregister Cisco Crosswork Network Controller.

Before you begin

Ensure that the product is in the **Registered** state.

Procedure

Step 1 From the main menu, choose **Administration** > **Smart Licenses** to display the **Smart licenses** tab.

Step 2 Click **Actions** and select the relevant option.

The available options include

- **Renew Authorization**—Use this option to renew the authorization manually if the automatic renewal fails at the end of 30 days.
- **Renew Registration**—Use this option to renew the registration manually if the automatic renewal fails at the end of six months.
- **Re-register**—Use this option to re-register the application, for example, if the registration tokens have expired.
- **De-register**—Use this option to deregister the application, for example, when you need to change the transport settings.

Note
Once deregistered, the application is moved to **Evaluation** mode (if the evaluation period is available) or **Evaluation Expired** mode.

Smart License Reservation

When Smart Licensing is used, Cisco Crosswork Network Controller shares usage information to CSSM at regular intervals. If you do not want to connect with CSSM regularly, Cisco Smart Licensing provides an option of offline reservation. It is useful in highly secure networks.

Cisco Crosswork Network Controller uses **Specific License Reservation (SLR)**, an enforced licensing model that is similar to node-locked licensing. SLR allows you to select only the required licenses. Anyone with a Smart Account can use the SLR feature if they have the product instances that support it.

Register Cisco Crosswork Network Controller with CSSM using offline reservation

Follow these steps to register Cisco Crosswork Network Controller with CSSM using offline reservation.

Before you begin

Ensure that you have a Smart Account. If not, go to Smart Account Request and follow the instructions on the website.

Procedure

Step 1 From the main menu, choose **Administration** > **Smart Licenses** to display the **Smart licenses** tab. The registration status and license authorization status displays **Unregistered** and **Evaluation mode** respectively.

Step 2 In the Smart Software Licensing information box at the top, click **Register**.

The Smart Software Licensing Product Registration dialog box appears. Select the **Register via Reserved License** radio button.

Step 3 Under the **Reservation code** section, click **Generate**. Your Reservation Request Code is generated and populated in the text field. Copy this code using the **Copy** option.

Step 4 Generate the Authorization Code in CSSM.

a) Log in to CSSM and select the appropriate Virtual Account.
b) Click the **Licenses** tab and then click **License Reservation**.
c) Paste the Reservation Request Code that you generated in Step 4 and click **Next**.
d) On the Select Licenses page, select the type of reservation you need. Then, click **Next**.
e) On the Review and Confirm page, click **Generate Authorization Code**. Copy the code using the **Copy to Clipboard** option.

Step 5 Navigate back to the Smart Software Licensing Product Registration page in the Cisco Crosswork Network Controller UI.

Step 6 Select the **Paste authorization code** option and paste the authorization code in the text field.

Step 7 Click **Register**.

It may take a few minutes to process the registration. Once completed, the registration status and license authorization status is updated as **Registered** and **Authorized** respectively.

Update offline reservation

Follow these steps to update the license counts reserved using offline reservation.

Procedure

Step 1 From the main menu, choose **Administration** > **Smart Licenses** to display the **Smart licenses** tab. Make a note of the Product Instance Name (available under the Smart software licensing status section).

Step 2 Generate the Authorization Code in CSSM.

a) Log in to CSSM and select the appropriate Virtual Account.
b) Navigate to the required product instance and click **Actions** > **Update Reservation**.
c) On the Select Licenses page, select the type of reservation you need. Then, click **Next**.
d) On the Review and Confirm page, click **Generate Authorization Code**. Copy the code using the **Copy to Clipboard** option.

Step 3 Navigate back to the Smart Software Licensing Product Registration page in the Cisco Crosswork Network Controller UI.

Step 4 Click **Actions** > **Update Reservation**.

Step 5 Paste the Authorization Code generated in Step 2 and click **Update**.

A Confirmation Code is generated. You can find this under the Smart Software Licensing Status section. Copy this code.

Step 6 Enter the Confirmation Code in CSSM.

a) Navigate back to CSSM and click the required product instance name.
b) Click the **Actions** > **Enter Confirmation Code**.
c) Enter or paste the Reservation Confirmation Code generated in Step 5 and click **OK**.

The license count will be updated in the Smart License page of the Cisco Crosswork Network Controller UI.

Disable offline reservation

Follow these steps to release the reserved licenses. Once the licenses are released, the application will be moved to **Evaluation** mode (if evaluation period is available) or **Evaluation Expired** mode.

Procedure

Step 1 From the main menu, choose **Administration** > **Smart Licenses** to display the **Smart licenses** tab. Make a note of the Product Instance Name (available under the Smart Software Licensing Status section).

Step 2 Click **Actions** > **Return Reservation**.

Step 3 In the Confirm Return Reservation window, click **Confirm**.

A Reservation Return Code (Release Code) is generated. Copy this code using the **Copy** option.

Step 4 Enter the Reservation Request Code in CSSM.

a) Log in to CSSM and select the appropriate Virtual Account.
b) Navigate to the required product instance and click **Actions** > **Remove**.
c) In the Remove Reservation dialog box, paste the Reservation Return Code generated in Step 3 and click **Remove Reservation**.

Step 5 Navigate back to the Smart License page in the Cisco Crosswork Network Controller UI. Notice that the Registration status has changed to **Unregistered**.

Step 6 Click **Actions** > **Disable License Reservation**.

License authorization status

This table describes the license authorization statuses based on the registration status.

Table 46: License authorization status

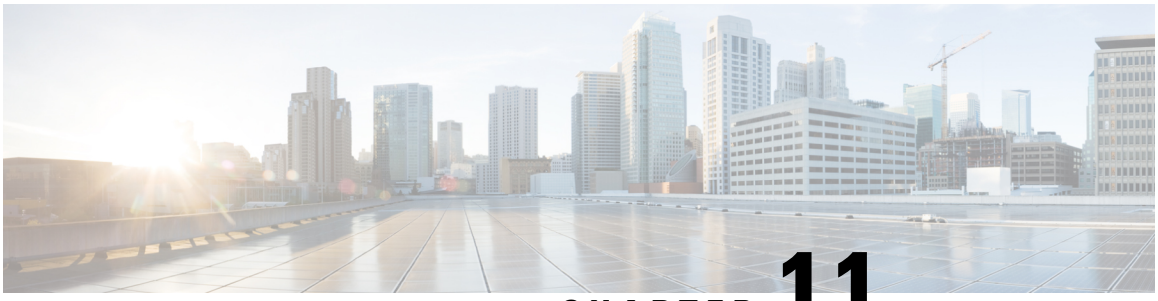
Registration status	License authorization status	Description
Unregistered	Evaluation mode	A 90-day evaluation period during which the licensed features of Cisco Crosswork Network Controller can be freely used. This state is initiated when you use Cisco Crosswork Network Controller for the first time.
	Evaluation Expired	Cisco Crosswork Network Controller has not been successfully registered at the end of the evaluation period. During this state, the Cisco Crosswork Network Controller features are disabled, and you must register to continue using the product.
	Registered Expired	Cisco Crosswork Network Controller is unable to contact the CSSM before the expiration of Identity Certificates and has returned to the unregistered state. Cisco Crosswork Network Controller resumes the remaining evaluation period, if available. At this stage, new registration ID token is required to reregister the product.
Registered	Authorized (In Compliance)	Cisco Crosswork Network Controller has been fully authorized to use the reserved licensed features. The authorization is automatically renewed every 30 days.
	Reserved (In Compliance)	Equivalent of "In Compliance" in offline reservation mode.
	Out of Compliance	The associated Virtual Account does not have enough licenses to reserve for Cisco Crosswork Network Controller’s current feature use. You must renew the entitlement or usage limit registered with the token to continue using Cisco Crosswork Network Controller.
	Not Authorized	Equivalent of "Out of Compliance" in offline reservation mode.
	Authorization Expired	Cisco Crosswork Network Controller is unable to communicate with the CSSM for 90 days or more, and the authorization has expired.

Authorization status responses

This table describes the actions or message enforced by Cisco Crosswork Network Controller in case of "Out of Compliance" or "Evaluation Expired" authorization status for Right-to-Use (RTU) and Right-to-Manage (RTM) licenses.

Table 47: Authorization status responses

Registration status	License authorization status	Enforced action or message
Registered	Out of compliance	No action taken.
Unregistered	Evaluation expired	All UI screens are disabled, and only the Smart Licensing window is displayed. An error message "Evaluation expired" is displayed. The UI remains blocked until a valid registration is completed.



CHAPTER 11

Manage Certificates

This chapter explains how to manage digital certificates by adding, editing, exporting, renewing, and updating them.

Certificates

A certificate is an electronic document that:

- identifies an individual, a server, a company, or entity
- associates the entity with a unique public key, and
- is digitally signed by an issuer (Certificate Authority or self-signed) to enable secure communication.

When a certificate is created with a public key, a matching private key is also generated. In TLS, the public key is used to encrypt data being sent to the entity and the private key is used to decrypt.

In a TLS exchange, a hierarchy of certificates is used to verify the validity of the certificate's issuer. This hierarchy is called a trust-chain and consists of 3 types of entities: a root CA certificate (self-signed), possibly multiple levels of intermediate CA certificates, and a server (or client) certificate (end-entity). The intermediate certificates act as a “link of trust” linking the server certificates to the CA’s root certificate and providing additional layers of security. The root certificate's private key signs and issues the next certificate in the chain. Subsequently, the private key for each certificate in the trust chain signs and issues the following certificate, continuing until the end entity certificate is signed. The end-entity certificate is the last certificate in the chain. It is used as a client or server certificate. For more details about these protocols, see *<xref to SSL in security hardening>* and *<xref to HTTPS in security hardening>*.

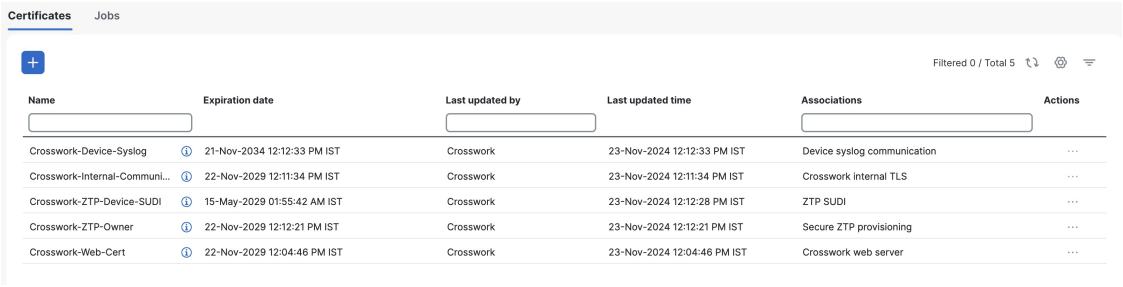
How are certificates used in Crosswork Network Controller?

Communication between Crosswork Network Controller applications and devices as well as between various Crosswork Network Controller components are secured using the TLS protocol. TLS uses X.509 certificates

to securely authenticate devices and encrypt data to ensure its integrity from source to destination. Crosswork Network Controller uses both generated certificates and certificates uploaded by clients . Uploaded certificates can be purchased from Certificate authorities (CA) or created as self-signed certificates. For example, the Crosswork Network Controller VM-hosted web server and the client browser-based user interface communicate with each other using Crosswork Network Controller generated X.509 certificates exchanged over TLS.

The Certificate Management window (**Administration** > **Certificate Management**) allows you to view, upload, and modify certificates. The following figure displays the default certificates provided by Crosswork Network Controller.

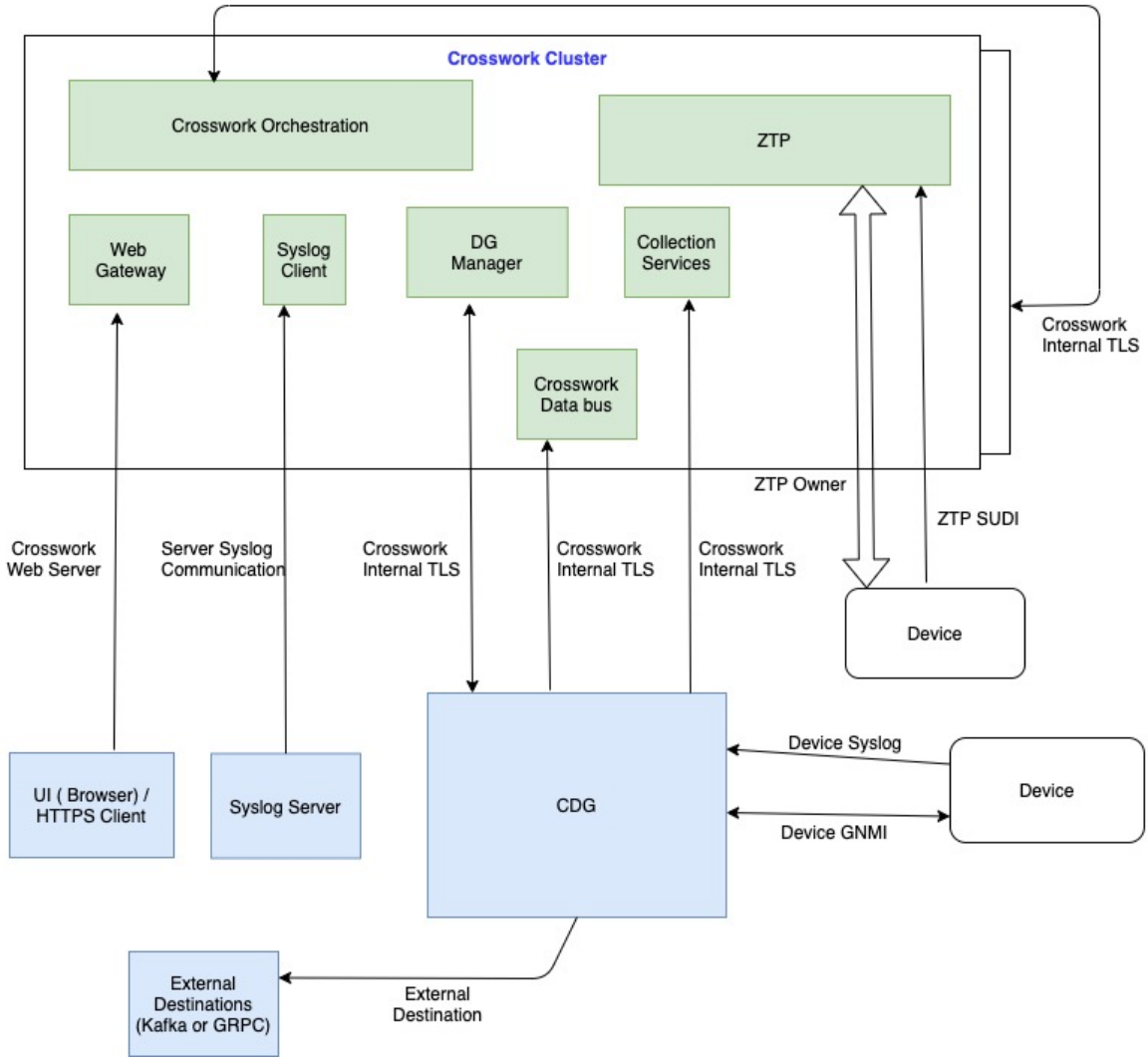
Figure 77: Certificate Management Window



Usage of certificate types

The following figure shows how Crosswork Network Controller uses certificates for various communication channels.

Figure 78: Certificates in Crosswork Network Controller



These certificates are classified into various roles with different properties depending on their use case as shown in the following table.

Table 48: Crosswork internal TLS certificate

Role	Crosswork internal TLS
UI Name	Crosswork-Internal-Communication

Description	• Generated and provided by Crosswork Network Controller. • This trust-chain is available in the UI (including the server and client leaf certificates) and is created by Crosswork Network Controller during initialization. They are used for interprocess communications between Crosswork Network Controller and Crosswork Data Gateway and communication between internal Crosswork Network Controller components. • Allows mutual and server authentication.
Server	Crosswork Network Controller
Client	Crosswork Data Gateway Crosswork Network Controller
Allowed operations	Download
Default expiry	5 years
Allowed expiry	—

Table 49: Device syslog communication certificate

Role	Device syslog communication
UI Name	Crosswork-Device-Syslog
Description	• Generated and provided by Crosswork Network Controller. • Provides Syslog telemetry communications between devices and Crosswork Data Gateway. • Allows server authentication.
Server	Crosswork Data Gateway
Client	Device
Allowed operations	Download
Default expiry	5 years
Allowed expiry	—

Table 50: ZTP SUDI certificate

Role	ZTP SUDI
UI Name	Crosswork-ZTP-Device-SUDI

Description	• A public Cisco certificate that is provided as part of Crosswork Network Controller. • Provides ZTP protocol communication channel between the ZTP application and device. • Allows server authentication.
Server	Crosswork ZTP
Client	Device
Allowed operations	• Upload • Download
Default expiry	100 years
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 51: Secure ZTP provisioning certificate

Role	Secure ZTP provisioning
UI Name	Crosswork-ZTP-Owner
Description	• Generated and provided by Crosswork Network Controller. • Forwarded by ZTP to devices and used for second layer of encryption.
Server	Crosswork ZTP
Client	Device
Allowed operations	• Upload • Download
Default expiry	5 years
Allowed expiry	31 days to 30 years. The validity period is user-defined.

Table 52: Crosswork web server certificate

Role	Crosswork web server
UI Name	Crosswork-Web-Cert

Description	• Generated and provided by Crosswork Network Controller. • Provides communication between the user browser and Crosswork Network Controller. • Allows server authentication.
Server	Crosswork Web Server
Client	User browser or API client
Allowed operations	• Upload • Download
Default expiry	5 years
Allowed expiry	Default expiry period is 5 years. Users can override this by uploading their own certificate. The allowed period is 31 days to 10 years.

Table 53: Provider gRPC communication certificate

Role	Provider gRPC communication
UI Name	—
Description	SR-PCE requires gRPC to discover topology and SR-MPLS policies. This certificate enables Transport Layer Security (TLS) and is required when the SR-PCE provider protocol is set to GRPC_SECURE.
Server	Crosswork Network Controller
Client	Clients that want secure connection to the gRPC server (Crosswork Data gateway, Device Group Manager pods, and so on)
Allowed operations	• Upload • Download
Default expiry	—
Allowed expiry	The validity period is user-defined.

Table 54: Device gNMI/gRPC communication certificate

Role	Device gNMI/gRPC communication
UI Name	—
Description	Provides GNMI telemetry communications between devices and Crosswork Data Gateway.
Server	Crosswork Data Gateway

Client	Device
Allowed operations	• Upload • Download
Default expiry	100 years
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 55: Server syslog communication certificate

Role	Server syslog communication
UI Name	—
Description	• Allows syslog events and logs from Crosswork Network Controller to an external Syslog server. • Allows server authentication.
Server	External syslog server
Client	Crosswork Network Controller
Allowed operations	• Upload **Note** You can upload multiple certificates associated with different servers. • Download
Default expiry	—
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 56: External destination certificate

Role	External destination
UI Name	—
Description	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a mutual-authentication.
Server	External Destinations (Kafka or gRPC)
Client	Crosswork Data Gateway

Allowed operations	• Upload **Note** You can upload one certificate and associate it with one or more external destinations. To upload multiple certificates, configure and select additional destinations. • Download
Default expiry	100 years
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 57: External destination server auth certificate

Role	External destination server auth
UI Name	—
Description	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a server-based authentication.
Server	External Crosswork Data Gateway Destinations (Kafka or gRPC)
Client	Crosswork Data Gateway
Allowed operations	• Upload **Note** You can upload one certificate and associate it with one or more external destinations. To upload multiple certificates, configure and select additional destinations. • Download
Default expiry	100 years
Allowed expiry	31 days to 100 years. The validity period is user-defined.

Table 58: Secure LDAP communication certificate

Role	Secure LDAP communication
UI Name	—
Description	Crosswork Network Controller uses the trust chain of this certificate to authenticate the secure LDAP server.
Server	Secure LDAP server
Client	Crosswork Network Controller

Allowed operations	• Upload **Note** You can upload multiple certificates associated with different servers. • Download
Default expiry	—
Allowed expiry	31 days to 30 years. The validity period is user-defined.

Table 59: Accedian provider mutual auth certificate

Role	Accedian provider mutual auth
UI Name	—
Description	Required to add provider connectivity assurance as a provider
Server	Provider
Client	Crosswork Network Controller
Allowed operations	• Upload • Download
Default expiry	—
Allowed expiry	31 days to 30 years. The validity period is user-defined.

There are two category roles in Crosswork Network Controller:

- Roles which allow you to upload or download trust chains only.
- Roles that allow upload or download of both the trust chain and an intermediate certificate and key.

Add a new certificate

This section explains the steps to add a new certificate. You can add certificates for these roles:

- **External destination**: Certificates uploaded for this role are used to secure communication between Crosswork Data Gateway and external destinations like Kafka servers. To enable mutual authentication, you upload a **CA Certificate Trustchain** that will be common to both Crosswork Data Gateway and the external server. This trust chain contains a root CA certificate and optional intermediate CA certificates. The last intermediate certificate in the chain and its corresponding private key are uploaded separately in the UI using **Intermediate key** , **Intermediate certificate** , and optionally **Passphrase** (if one was used for generating the intermediate key). Crosswork Network Controller internally creates a client certificate using this intermediate key for Crosswork Data Gateways that connect to the external destination. The destination server certificate trust, such as Kafka, must be derived from the same root CA certificate.

You can upload certificates to the **External Destination** role, the authentication type must be opted as **Mutual-Auth** on the **Add Destination** page. For more information about the authentication types, see Add or edit a data destination, on page 92.

- **Server Syslog Communication**: You upload the trust chain of the Syslog server certificate. This trust chain is used by Crosswork Network Controller to authenticate the Syslog server. After this trust chain is uploaded and propagated within Crosswork Network Controller, you can add the syslog server (**Administration** > **Settings** > **Syslog Server Configuration**) and associate the certificate to enable TLS. For more information, see Configure a Syslog Server.
- **Device gNMI/gRPC communication**: You upload a bundle of trust chains used by Crosswork Data Gateway to authenticate the devices connecting to it. This trust chain and the device gNMI certificate must also be configured on the device. The trust chain file that is uploaded can contain multiple hierarchies of trust certificates as needed to allow all the devices in the network to connect. For more information, see Add the gNMI certificate, on page 148.
- **Secure LDAP communication**: You upload the trust chain of the secure LDAP certificate. This trust chain is used by Crosswork to authenticate the secure LDAP server. Once this trust chain is uploaded and propagated within Crosswork Network Controller, you can add the LDAP server and associate the certificate.
- **External destination server auth**:
  - Upload the root CA certificate to establish secure communication between the Crosswork Data Gateway and external destinations, such as Kafka servers.
  - You can upload certificates to the **External Destination Server Auth** role only when the authentication type is set to **Server-Auth**.
  - You can upload certificates for the Crosswork Data Gateway, applications, or both using the same role by selecting the appropriate data destination type.
  - The **Data source** field in the data destination form indicates whether the destination applies to the Crosswork Data Gateway, applications, or both.
- **Provider gRPC communication**: You upload a well-known CA certificate trust chain bundle for secure communication between Crosswork Network Controller and gRPC server configured on an external SR-PCE provider. Mutual authentication is currently not supported.

Note Crosswork Network Controller does not receive a web certificate directly. It accepts an intermediate CA and intermediate Key to create a new web certificate, and apply it to the Web Gateway.

If you prefer to upload your own ZTP and web certificates (instead of using the default certificates provided within Crosswork Network Controller), use the Edit function (see Edit certificates, on page 379).

Before you begin

- Upload all certificates in Privacy Enhanced Mail (PEM) format. Also, note the location of the certificates on the system for easy navigation.
- Uploaded Trust chain files may contain the entire hierarchy (root CA and intermediate certificates) in the same file. In some cases, multiple chains are also allowed in the same file.
- Ensure the intermediate keys are either in PKCS1 or PKCS8 format.

- Configure a data destination before you add a new certificate for an external destination. For more information, see Add or edit a data destination, on page 92.
- Ensure there are no collection jobs configured for destinations when adding or updating a certificate with multiple destinations.
- Ensure that the *tyk* service is in a healthy state.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management** and click  .

Step 2 Enter a unique name for the certificate.

Step 3 From the **Certificate Role** drop-down, select the purpose for which the certificate is to be used. For more information, see Usage of certificate types , on page 370.

Note
You can select available destinations (Kafka/gRPC) while adding or updating an **External Destination** certificate.

Step 4 Click **Browse** , and navigate to the certificate trustchain.

Step 5 In the case of an **External Destination** certificate, you must select one or more destinations and provide the CA certificate trustchain, intermediate certificate, and intermediate key. The passphrase field is optional and is used to create the intermediate key (if applicable).

Step 6 Click **Save**.

Note
After you upload the certificate, the Crosswork Cert manager accepts it, validates it, and generates the server certificate. Upon successful validation, an alarm ("Crosswork Web Server Restart") indicates that the certificate is about to be applied. The Certificate Management UI then logs out automatically and applies the certificate to the Web Gateway. The new certificate can be checked by clicking the lock <Not Secure>/<secure> icon next to the https://<crosswork_ip>:30603.

Related Topics

Usage of certificate types , on page 370
Add or edit a data destination, on page 92

Edit certificates

Crosswork Network Controller allows you to update web certificates by importing an intermediate Certificate Authority (CA) certificate. You can edit certificates to add or remove connection destinations, and upload or replace expired or misconfigured certificates. This applies to user-provided certificates , ZTP certificates, and web certificates. However, you cannot modify the system certificates provided by Cisco Crosswork. These certificates will not be available for selection.

Crosswork Network Controller also allows you to configure the client authentication for web certificates. Client authentication offers an alternative method for setting up user authentication in Crosswork. It requires both the client and server to present digital certificates to verify their identities. Enabling this feature can provide a more seamless login experience for users.

You can also remove a certificate by following this procedure to replace the certificate or by disabling security (**Enable Secure Communication**) option for any assigned destinations (see Add or edit a data destination, on page 92). You cannot permanently delete a certificate from the Crosswork system.

Before you begin

- Updating the certificate can disrupt the existing trust chain of certificates used for client authentication if enabled, so proceed with caution.
- Restart Crosswork server during this process. The restart will take several minutes to complete.
- Set the AAA mode to Local to enable client authentication.

Procedure

Step 1 Choose **Administration** > **Certificate Management** to view the **Certificate Management** window.

Step 2 To update a certificate:

a) Under the **Actions** column, click ... on the certificate that you want to modify, and select **Update certificate** .

b) Enter the appropriate values for the fields based on the certificate you wish to update. Click the icon next to the field for more information.

c) Click **Save** to save the changes.

Step 3 To enable the client certificate authentication of a web certificate:

a) Under the **Actions** column, click ... on the Crosswork web certificate that you want to modify, and select **Configure client certificate authentication** .

The **Configure Client Authentication** window is displayed.

b) Check the **Enable** checkbox.

The **Certificate schema** and **OCSP** settings are displayed.

The **OCSP** settings are enabled by default, but you can disable them if you prefer. When these settings are enabled, you can check the certificate revocation status using the Online Certificate Status Protocol (OCSP).

c) Choose the **Certificate schema** value.

- **Automatic** —Searches for the user principal name (UPN) in the alternate subject name area. If a UPN is not found, the system will use the common name value. This is the default selection.
- **Manual** —Searches for the username in the subject area based on the user identity source and the specified regular expression.

d) (Optional) Choose the **OCSP** value:

- **Automatic** —Extracts the responder URL from the certificate and uses it to perform OCSP validation.
- **Manual** —You must provide the OCSP responder URL.

e) Click **Save** to save the changes.

Step 4 To update certificate and configure client authentication in a single step:

a) Click ··· on the Crosswork web certificate that you want to modify, and select **Update certificate & config. client cert. authentication** .

The **Update Certificate and Configure Client Authentication** window is displayed.

Note
Choosing the combined option to update the certificate and configure client authentication minimizes downtime during the Crosswork server restart, as it occurs only once instead of twice if these actions are performed separately.

b) Enter the data as per the instructions described in step 2 and step 3.
c) Click **Save** to save the changes.

Download certificates

To export certificates, perform these steps:

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management**.

Step 2 Click ⓘ for the certificate you want to download.

Step 3 To separately download the root certificate and the intermediate certificate, click ⬆ next to the certificate. To download the certificates at once, click **Export All**.

Renew certificates

Kubernetes certificate renewal

Certificates are valid for one year before they expire. After you renew the certificates, ensure that the pods are healthy before resuming other operations.

Note If you renew certificates before they expire, it is recommended to perform this activity during a maintenance window to keep the cluster in an operational state.

To renew a certificate, perform these steps:

Before you begin

- Create a plain text file on your local machine (for example, `password.txt`) that contains the SSH login password for the server.
- Keep the management IP addresses readily available for the hybrid and worker nodes in your cluster.

Procedure

Step 1 Create a backup of your Crosswork Network Controller.

Step 2 Log in to one of your hybrid nodes.

Step 3 Renew the Kubernetes certificates using the `renew_k8s_cert` command. The required parameters depend on whether the certificates have already expired.

- **Before certificate expiry** : If the certificates have not yet expired, you can renew them by running the following command. You do not need to specify the hybrid or worker node management IP addresses.

  ```
  renew_k8s_cert --user=<ssh-username> --passwdfile=<passfile-path>
  ```

  Example:

  ```
  renew_k8s_cert --user=cw-admin --passwdfile=/home/cw-admin/password.txt
  ```

- **After certificate expiry** : If the Kubernetes certificates have already expired, you must specify the management IP addresses of the hybrid and (if applicable) worker nodes in your cluster.

  ```
  renew_k8s_cert --hybrid=hybridNodeMgmtIP1,hybridNodeMgmtIP2,hybridNodeMgmtIP3
                                 --worker=workerNodeMgmtIP1,workerNodeMgmtIP2,workerNodeMgmtIP3
  --user=<ssh-username> --passwdfile=<passfile-path>
  ```

  Replace the parameters as follows:

  - **hybridNodeMgmtIP** : Management IP of each hybrid node (comma-separated).
  - **workerNodeMgmtIP** : Management IP of each worker node (comma-separated, optional if you have no worker nodes).
  - **ssh-username** : The SSH username to use.
  - **passfile-path** : Path to the plain text file containing the SSH login password.

  IPv4 example for a 6-node cluster:

  ```
  renew_k8s_cert --hybrid=10.10.10.101,10.10.10.102,10.10.10.103
                                 --worker=10.10.10.104,10.10.10.105,10.10.10.106 --user=cw-admin

                                 --passwdfile=/home/cw-admin/password.txt
  ```

  IPv4 example for a 3-node cluster (hybrid nodes only):

  ```
  renew_k8s_cert --hybrid=10.10.10.101,10.10.10.102,10.10.10.103 --user=cw-admin
                                 --passwdfile=/home/cw-admin/password.txt
  ```

  IPv4 example for single VM deployment:

  ```
  renew_k8s_cert --hybrid=10.10.10.101 --user=cw-admin --passwdfile=/home/cw-admin/password.txt
  ```

  IPv6 example for a dual-stack cluster:

  ```
  renew_k8s_cert --hybrid=fded:1bc1:fc3e:96d0:192:168:5:451,fded:1bc1:fc3e:96d0:192:168:5:452,
                                 fded:1bc1:fc3e:96d0:192:168:5:453
  --worker=fded:1bc1:fc3e:96d0:192:168:5:454,fded:1bc1:fc3e:96d0:192:168:5:455
                                 --user=cw-admin --passwdfile=/home/cw-admin/password.txt
  ```

Attention

- The `--worker` parameter is optional if you do not have worker nodes in your cluster.
- Line breaks in the commands above are for display only. Remove all line breaks before executing the command.

Step 4 (Optional) **Recover cluster:** If multiple pods are stuck in `ContainerCreating` or `terminating` state after you renew the Kubernetes certificate, run these commands on any hybrid node.

```
kubectl delete pod -n kube-system -l k8s-app=calico-kube-controllers --grace-period=0 --force
```

Wait for the `calico-kube-controllers` pods to start, and run this command:

```
kubectl delete pod -n kube-system -l k8s-app=calico-node --grace-period=0 --force
```

After all the Calico pods are up and running, all other pods will recover and enter a running state. If any pods remain in a non-running state, wait at least 10 minutes after the Calico pods started, and then run this command:

```
kubectl get po --all-namespaces | awk '{if ($4 != "Running") system ("kubectl -n " $1 " delete pods
 " $2 " --grace-period=0 " " --force ")}'
```

Automatic renewal of internal certificates

Crosswork CA generates TLS certificate chains, including root, intermediate CA, and leaf certificates, for day 0 deployments (Geo HA and non-Geo HA). The leaf certificates are valid for 2 years, while root and intermediate CA certificates are valid for 5 years. Customers with Crosswork deployments lasting beyond two years will face certificate expiry. This expiry disrupts TLS communication and impacts cluster operations. Auto-renewal applies to all Crosswork certificates generated internally, including NATS, Kafka, and any application-specific internal certificates.

The renewal alert is generated only when the expiry period is less than 90 days. When an internal certificate is expiring and renewed, all internal certificates of that type will be renewed. For example, when a leaf certificate is renewed, the process will also renew all other leaf certificates.

Important **For geo HA deployment:**

- For a Geo HA deployment, the certificate renewal is triggered in the active AZ cluster. The TLS manager determines if the cluster has geo redundancy enabled or disabled and decides whether the certificate renewal must be performed on one cluster or both geo HA clusters. After the renewal job is completed on the active cluster, the job automatically runs in the standby cluster after a delay. The standby cluster then displays job progress and alarm events.

  In a Geo HA setup with auto-arbitration, the certificate is first renewed on the active cluster, then simultaneously renewed on the standby cluster and the arbiter VM.

The certificate renewal process can cause a downtime of approximately thirty minutes to one hour. It is recommended to perform this activity during a maintenance window to avoid disrupting cluster operations.

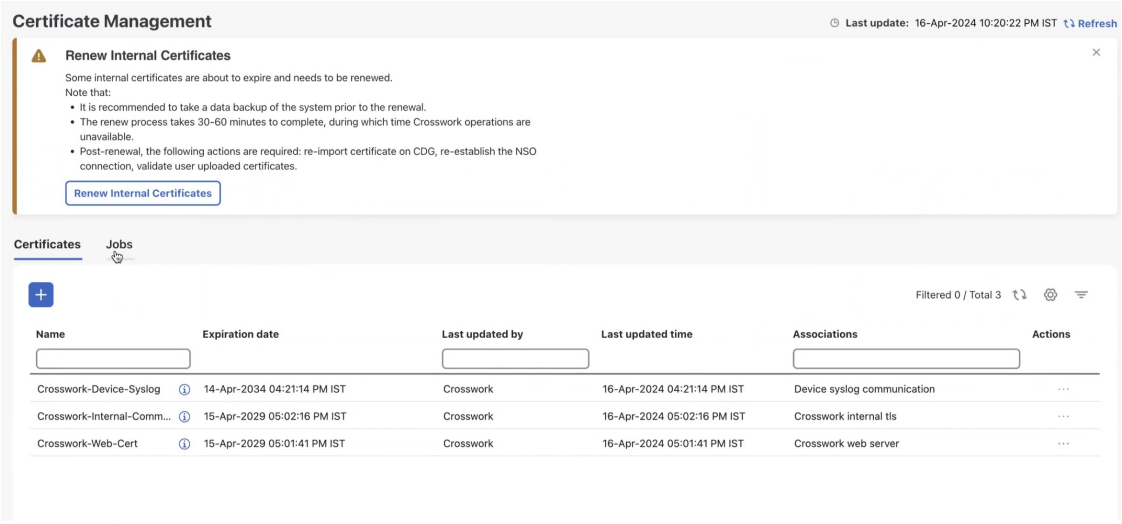
To renew an internal certificate, perform the following:

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management**. The **Certificate Management** window appears. If an internal certificate is about to expire, a prompt appears for certificate renewal.

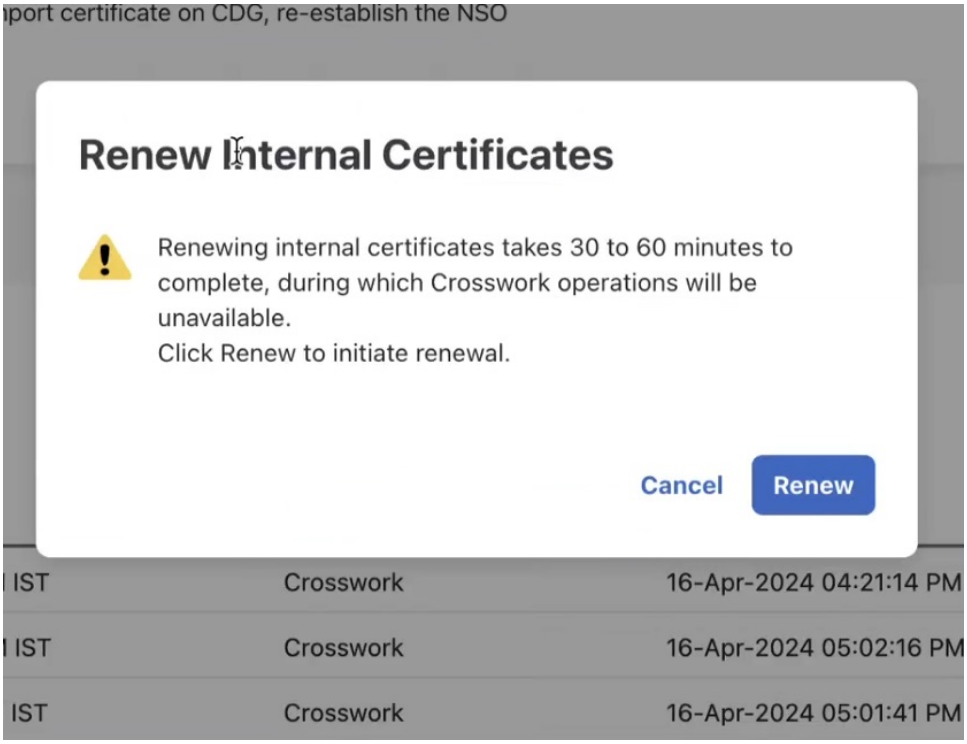
Note
The Crosswork dashboard displays alerts about certificate expiry when you log in. The system generates alerts at various stages of the certificate expiry, increasing severity as the expiry date approaches.

Figure 79: Renew Internal Certificate prompt



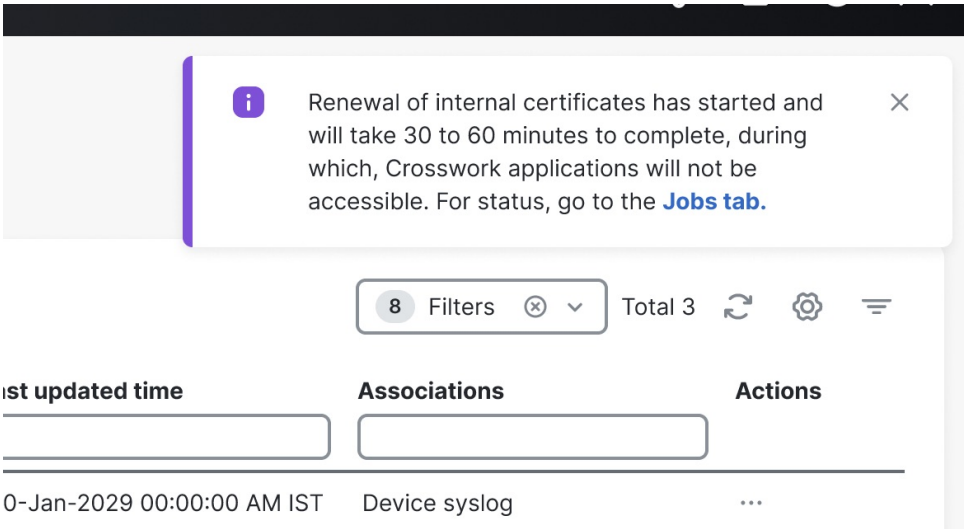
Step 2 Click **Renew Internal Certificate** . A confirmation popup is displayed. Click **Renew** to confirm.

Figure 80: Renewal Confirmation Prompt



This action invokes the REST API (/v2/cert/renew) and initiates the certificate expiry check. The **Certificate Management** window displays a notification about the new renewal job.

Figure 81: Renewal Job Notification



You can view progress of the renewal job from the **Jobs** tab. After the job completes, an Info alarm event indicates successful completion of the job. You must manually clear this alarm to acknowledge the event. Any error during the process will result in job failure. However, the job can be triggered again because the API is repeatable.

Step 3 **In case of Geo HA deployment**: After successfully completing the certificate renewal, run an on-demand or periodic sync across the active and standby clusters to ensure that asynchronous replication is re-established over a secure channel.

Step 4 After the renewal job completes, perform these steps to maintain TLS communication between Crosswork and other external components:

a) **Crosswork with Crosswork Data Gateway**: When Crosswork certificates are renewed, it automatically pushes the updated certificates to each Crosswork Data Gateway. During the update process, Crosswork raises alarms for each Data Gateway to indicate these events:

- Certificate update started
- Certificate update completed

Note
The automatic certificate renewal happens as part of the Crosswork Data Gateway day-N enablement process.

b) **In case of Geo HA deployment:**

- The automatic certificate renewal process starts when the certificates are updated. After DG-Manager pushes the updated certificates to the Data Gateway, all the affected Data Gateways automatically restart. The restart causes a brief service interruption.
- If certificate renewal fails, the Crosswork Data Gateway enters error state after the DG-Manager restarts. To recover, manually reimport the certificates on the affected Data Gateway. For more information, see Import a certificate, on page 488.

c) **Crosswork Data Gateway and Device Syslog**: If device syslog root and intermediate certificates are renewed, manually export and reconfigure these certificates on all devices. For internally generated Crosswork CA certificates, export the new device syslog root and intermediate CA certificates and configure them as CA trustpoints on IOS XR/XE devices. For more information, see the IOS XE and IOS XR instructions in Syslog collection jobs, on page 132.

If there is a renewal for device syslog root and intermediate certificates, manually export these certificates to the devices.

d) **External destination/Server Auth CA** : Re-upload the External Destination and Server Auth CA certificates to Crosswork.

e) **Cisco NSO**: Export the regenerated Crosswork Web server certificate from the Crosswork UI browser, configure it, and store it on the NSO server. For more information, see the Step 1b in the *<xref to Configure standalone NSO topic>* section.

Update the web certificate using a certificate signing request

Update the web certificate to use one signed by an Enterprise or Commercial CA, without exposing the private key outside Crosswork Network Controller.

Starting with version 7.0.1, Crosswork Network Controller enables updating web certificates via a Certificate Signing Request (CSR) to enhance trust and security.

Before you begin

- Updating the certificate can disrupt the existing trust chain of certificates used for client authentication if enabled, so proceed with caution.
- This process requires the Crosswork server to be restarted, which will take several minutes to complete.
- Set the AAA mode to Local to enable client authentication.

Procedure

Step 1 From the main menu, choose **Administration** > **Certificate Management**

Step 2 Click ··· on the web certificate (`Crosswork-Web-Cert`) and select **Update Certificate** .

The **Certificate Update Method** window appears.

Step 3 Create a CSR to submit to the Certificate Authority.

a) Select **Create a certificate signing request (CSR)** radio button and click **Update certificate** .

The **Certificate Signing Request (CSR)** window appears.

b) Click **Create CSR** .

The **Create Certificate Signing Request (CSR)** window appears.

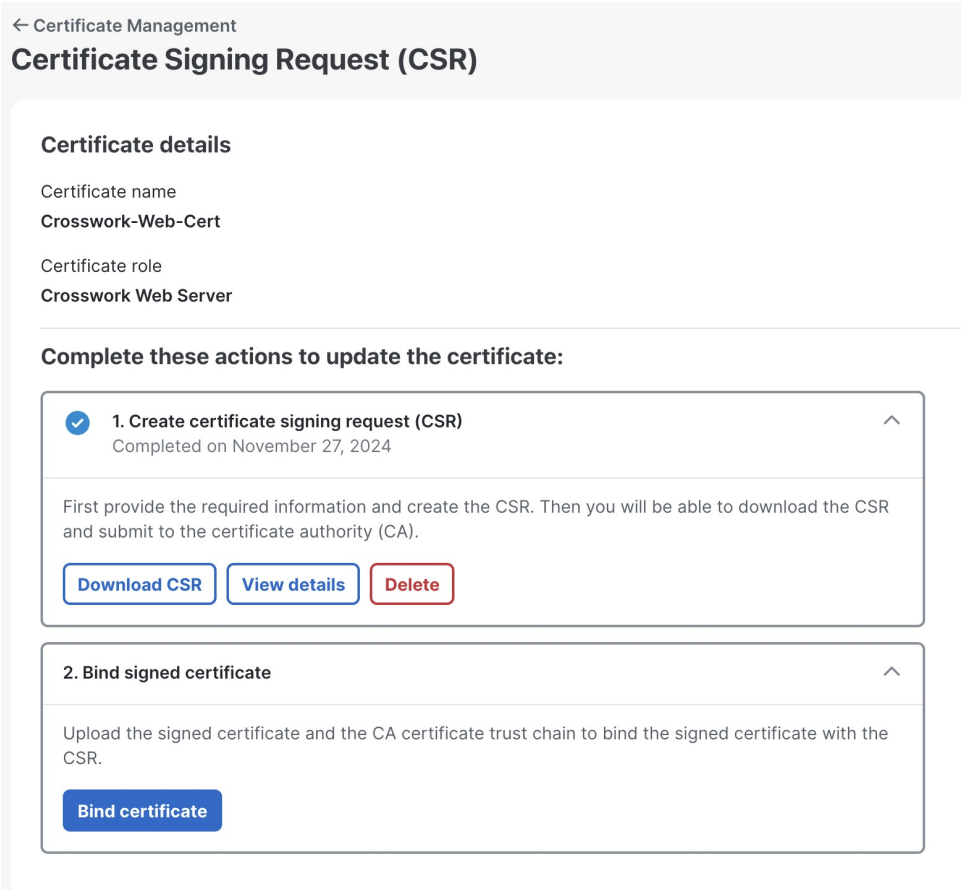
c) Enter the required relevant values for the fields. Click the ⓘ icon next to the field for more information. The mandatory fields are:

- **Common name (CN)**: By default, this is the fully qualified domain name (FQDN) of the server, but it can be any unique name that identifies the server. The length should not exceed 64 characters.
- **IP address**: This is the Crosswork VIP address used in this deployment. Additional IP addresses should only be added if necessary for certificate validation.
- **Key type**: The options are RSA and ECDSA. By default, RSA is selected.
- **Key size (in bits)**: The options are 2048, 3072, and 4096. By default, 2048 is selected.
- **Key digest**: The options are SHA-256, SHA-384, SHA-224, and SHA-512. By default, SHA-256 is selected.

d) Click **Create CSR** to complete the action.

Step 4 After generating the CSR, click **Download** to download it and use the CSR to get a signed certificate from your CA.

Figure 82: Certificate Signing Request (CSR) window

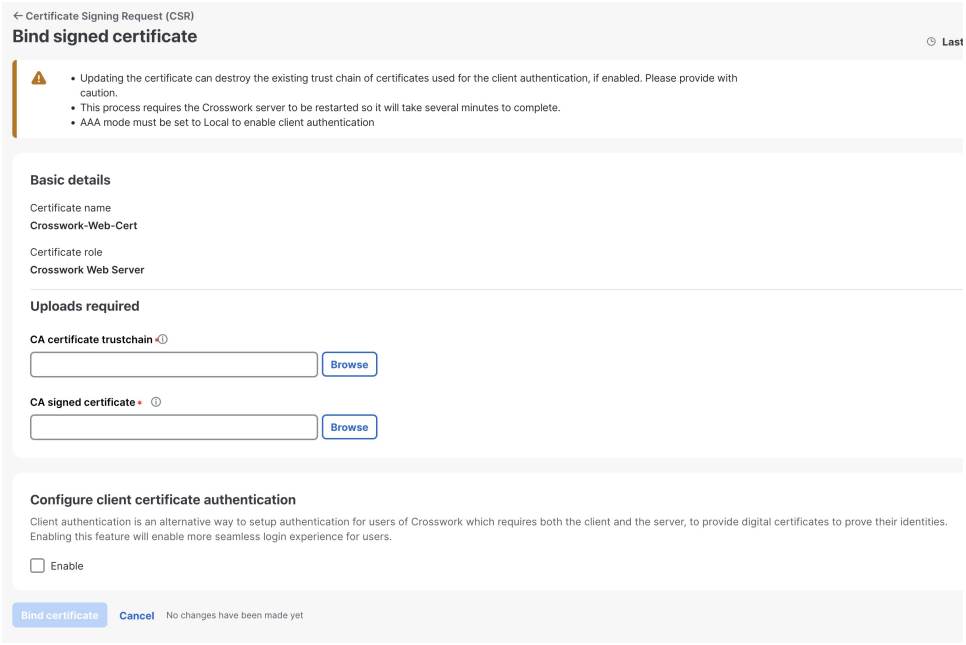


Step 5 Upload the CA-signed certificate and CA certificate trustchain to bind the certificate.

a) In the **Certificate Signing Request (CSR)** window, click **Bind certificate** .

The **Bind signed certificate** window is displayed.

Figure 83: Bind signed certificate

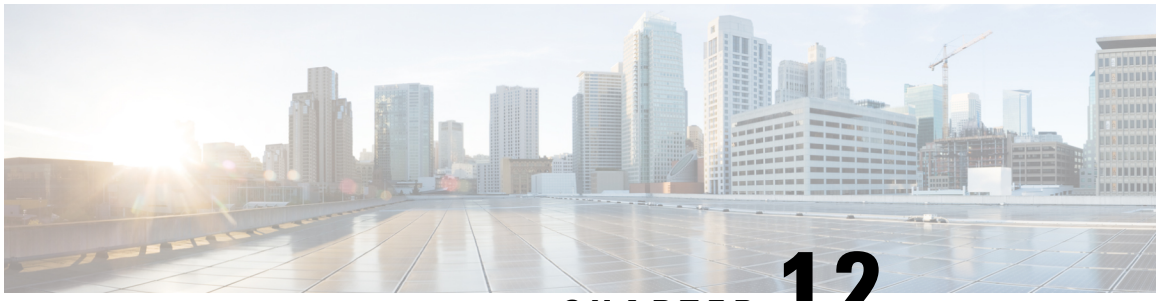


b) Upload the relevant data for the fields provided. Click the ⓘ icon next to the field for more information.
   - **CA certificate trustchain**: This is the certificate trust chain for the web server certificate obtained from the CA.
   - **CA signed certificate**: This is the final signed certificate for the web server obtained from the CA.

c) (Optional) Click the **Enable** checkbox to configure client certificate authentication.
d) Click **Bind certificate** to complete the operation.

   After the bind action is completed, the web certificate is updated. Tyk will then restart with the new web certificate.

The Crosswork Network Controller's web certificate is updated with the CA-signed certificate and trust chain after server restart.



CHAPTER 12

Manage System Access and Security

This section contains the following topics:

Manage Users

As a best practice, administrators should create separate accounts for all users. Prepare a list of the people who will use Cisco Crosswork. Decide on their user names and preliminary passwords, and create user profiles for them. During the creation of a user account, you assign a user role to determine the functionality to which the user will have access. If you will be using user roles other than "admin", create the user roles before you add your users (see Create User Roles, on page 394).

You can optionally view the NETCONF Access Control Model (NACM) rules that let admin members grant access to devices in selected groups and deny access to other devices.

Procedure

Step 1 From the main menu, select **Administration** > **Users and Roles** > **Users** tab. From this window, you can add a new user, edit the settings for an existing user, and delete a user.

Step 2 To add a new user:

a) Click  and enter the required user details.

When you are configuring Device Access Groups for your users, select the **Device Access Group** listed in the right pane to assign it to the new user you are creating.

Note

1. By default users associated with ALL-ACCESS Device Access Group are provided access to ALL devices.
2. You must associate at least one Device Access Group to a user.

b) Click **Save**.

Step 3 To edit a user:

a) Click the checkbox next to the User and click .
b) After making changes, click **Save**.

Step 4 To delete a user:

a) Click the checkbox next to the User and click .
b) In the **Confirm Deletion** window, click **Delete**.

Step 5 To view the audit log for a user:

a) Click the icon under the **Actions** column, and select **Audit Log**.

The **Audit Log** window is displayed for the selected user name. For more information on the Audit Logs, see View Audit Log, on page 475.

Step 6 (Optional) To view NACM rules for a user:

a) Click the icon under the **Actions** column, and select **Generate NACM Rules**.

The **NACM Rules** window is displayed for the selected user name.

If you have an NSO service configured on your Crosswork Network Controller, you can generate NACM rules by clicking the icon under the **Actions** column for a user and selecting **Generate NACM Rules**. This will integrate device-level NACM control with the NSO workflow. Note that for each unique combination of Device Access Group associated with a user, there is:

- A NACM group associated with the user.
- A corresponding NACM rule list associated with the user.

The rule will allow access to devices in selected Device Access Groups and deny access to other devices. You can copy the XML rules file and add it in your NSO NACM Rule configuration setup. The options available under the NSO Actions tab, located in Device **Management > Network Devices**, will also be restricted based on the Device Access Groups permissions of the user.

You also view the Crosswork Audit log and the NSO commit logs to track and verify the activities of users using the NACM rules, ensuring traceability.

Administrative Users Created During Installation

During installation, Crosswork creates two special administrative IDs:

1. The **virtual machine administrator**, with the username **`cw-admin`**, and the default password **`admin`**. Data center administrators use this ID to log in to and troubleshoot the VM hosting the Crosswork server.
2. The **Cisco Crosswork administrator**, with the username **`admin`** and the default password **`admin`**. Product administrators use this ID to log in to and configure the user interface, and to perform special operations, such as creating new user IDs.

The default password for both administrative user IDs must be changed the first time they are used.

User Roles, Functional Categories and Permissions

The **Roles** window lets users with the appropriate privileges define custom user roles. As with the default *admin* role, a custom user role consists of:

- A unique name, such as “Operator” or “admin”.
- One or more selected, named functional categories, which control whether or not a user with that role has access to the APIs needed to perform specific Cisco Crosswork functions controlled by that API.
- One or more selected permissions, which control the scope of what a user with that role can do in the functional category.

For a user role to have access to a functional category, that category and its underlying API must show as selected on the **Roles** page for that role. If the user role shows a functional category as unselected, then users with this role assigned will have no access to that functional area at all.

Some functional categories group multiple APIs under one category name. For example: The “AAA” category controls access to the Password Change, Remote Authentication Servers Integration, and Users and Role Management APIs. With this type of category, you can deny access to some of the APIs by leaving them unselected, while providing access to other APIs under the category by selecting them . For example: If you want to create an “Operator” role who is able to change his own password, but not see or change the settings for your installation’s integration with remote AAA servers, or create new users and roles, you would select the “AAA” category name, but uncheck the “Remote Authentication Server Integration API” and “Users and Role Management API” checkboxes.

For each role with a selected category, the **Roles** page also lets you define permissions to each underlying functional API:

- **Read** permission lets the user see and interact with the objects controlled by that API, but not change or delete them.
- **Write** permission lets the user see and change the objects controlled by that API, but not delete them.
- **Delete** permission gives the user role delete privileges over the objects controlled by that API. It is useful to remember that delete permission does not override basic limitations set by the Crosswork platform and it applications.

Although you can mix permissions as you wish:

- If you select an API for user access, you must provide at least “Read” permission to that API.
- When you select an API for user access, Cisco Crosswork assumes that you want the user to have all permissions on that API, and will select all three permissions for you, automatically.
- If you uncheck all of the permissions, including “Read”, Cisco Crosswork will assume that you want to deny access to the API, and unselect it for you.

Best Practices:

Cisco recommends that you follow these best practices when creating custom user roles:

- Restrict **Delete** permissions in roles for *admin* users with explicit administrative responsibility for maintenance and management of the Crosswork deployment as a whole.

- Roles for developers working with all the Cisco Crosswork APIs will need the same permissions as *admin* users.
- Apply at least **Read** and **Write** permissions in roles for users who are actively engaged in managing the network using Cisco Crosswork.
- Give read-only access to roles for users who only need to see the data to help their work as system architects or planners.

The following table describes some sample custom user roles you should consider creating:

Table 60: Sample custom user roles

Role	Description	Categories/API	Privileges
Operator	Active network manager, triggers Playbooks in response to KPI alerts	All	Read, Write
Monitor	Monitors alerts only	Health Insights, Inventory, Topology	Read only
API Integrator	All	All	All

Note Admin role needs to include permissions for Read, Write, and Delete, while read-write roles need to include both Read and Write permissions. Using Zero Touch Provisioning features requires access to all ZTP APIs.

Create User Roles

Procedure

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

The **Roles** window has a **Roles** table on the left side and a corresponding **Global API Permissions** tab on the right side which shows the grouping of user permissions for the selected role.

Step 2 On the **Roles** table, click  to display a new role entry in the table.

Step 3 Enter a unique name for the new role.

Step 4 To define the user role's privilege settings, select the **Global API Permissions** tab and perform the following:

a) Check the check box for every API that users with this role can access. The APIs are grouped logically based their corresponding application.

b) For each API, define whether the user role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 5 Click **Save** to create the new role.

To assign the new user role to one or more user IDs, edit the **Role** setting for the user IDs (see Edit User Roles, on page 395).

Clone User Roles

Cloning an existing user role is the same as creating a new user role, except that you need not set privileges for it. If you like, you can let the cloned user role inherit all the privileges of the original user role.

Cloning user roles is a handy way to create and assign many new user roles quickly. Following the steps below, you can clone an existing role multiple times. Defining the cloned user role's privileges is an optional step; you are only required to give the cloned role a new name. If you like, you can assign it a name that indicates the role you want a group of users to perform. You can then edit the user IDs of that group of users to assign them their new role (see Manage Users, on page 391). Later, you can edit the roles themselves to give users the privileges you want (see Edit User Roles, on page 395).

Note Some API permissions are predefined in the system admin role and remain unchanged in the cloned role. For example, the system admin role includes the default **Read** and **Write** permissions for the **Alarms & Events** API. These permissions are not configurable for both, original, and cloned admin roles.

Procedure

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

Step 2 Click an existing role.

Step 3 Click to create a new duplicate entry in the **Roles** table with all the permissions of the original role.

Step 4 Enter a unique name for the cloned role.

Step 5 (Optional) Define the role's settings:

a) Check the check box for every API that the cloned role can access.

b) For each API, define whether the clone role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 6 Click **Save** to create the newly cloned role.

Edit User Roles

Users with administrator privileges can quickly change the privileges of any user role other than the default **admin** role.

Procedure

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

Step 2 Click and select on an existing role from the left side table. The **Global API Permissions** tab on the right side displays the permission settings for the selected role.

Step 3 Define the role's settings:

a) Check the check box for every API that the role can access.

b) For each API, define whether the role has **Read**, **Write**, and **Delete** permission by checking the appropriate check box. You can also select an entire API group (such as AAA), and all the APIs under the group will be selected with **Read**,**Write** and **Delete** permissions pre-selected.

Step 4 When you are finished, click **Save**.

Delete User Roles

Users with administrator privileges can delete any user role that is not the default **admin** user role or that is not currently assigned to a user ID. If you want to delete a role that is currently assigned to one or more user IDs, you must first edit those user IDs to assign them to a different user role.

Procedure

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

Step 2 Click on the role you want to delete.

Step 3 Click  .

Step 4 Click **Delete** to confirm that you want to delete the user role.

Global API Permissions

The **Roles** window lets users with the appropriate privileges define custom user roles.

The following table is an overview of the various **Global API Permissions** in Cisco Crosswork:

Table 61: Global API Permission Categories

Category	Global API Permissions	Description
AAA	Password Change	Provides permission to manage passwords. The READ and WRITE permissions are automatically enabled by default. The DELETE permission is not applicable to the password change operation (You cannot delete a password, you can only change it.)
	Remote Authentication Servers Integration	Provides permission to manage remote authentication server configurations in Crosswork. You must have READ permission to view/read configuration, and WRITE permission to add/update the configuration of any external authentication server (e.g. LDAP, TACACS) into Crosswork. The Delete permissions are not applicable for these APIs.
	Users and Roles Management	Provides permission to manage users, roles, sessions, and password policies. Supported operations include "Create new user/role", "Update user/role", "Delete a user/role", "Update task details for a user/role", "Session management (Idle-timeout, max session..)", "update password policy", "get password tooltip help text", "get active sessions", etc. The READ permission allows you to view the content. The WRITE permission allows you to create and update. The DELETE permission allows you to delete a user or role.
	Know my role - Read only	Enables the logged in users to understand their permissions, or get new permissions. WRITE and DELETE permissions are not applicable for these APIs.
	User Preferences	Allows you to manage the dashlets in the homepage. The READ permission allows you to view dashboards, WRITE permission allows your to edit dashboards, DELETE permission allows you to delete dashboards.
Administrative Operations	External Notification Subscription	Allows you to subscribe or unsubscribe the external kafka notification streaming. The READ permission allows you to view the list of subscriptions. The WRITE and DELETE permissions allows you to edit and delete the subscriptions respectively.
	RESTCONF Notification Subscription	Allows you to subscribe or unsubscribe the RESTCONF notification streaming (websocket and connectionless). The READ permission allows you to view the list of subscriptions. The WRITE and DELETE permissions allows you to edit and delete the subscriptions respectively.

Category	Global API Permissions	Description
Device Monitoring	Device Inventory RESTCONF	Responsible for the retrieving the inventory information. The READ permission allows you to get all the inventory data such as nodes,termination points, equipments, and modules. The WRITE and DELETE permissions are not applicable for this API as there is no support for configuration-related operations.
	Performance Monitoring Dashboards	The READ permission allows displaying any metrics on the Crosswork Network Controller homepage, dashboard window, and deep inventory. The WRITE and DELETE permissions are not applicable for this API.
	Performance Monitoring Policies	Allows you to manage monitoring policies. The READ permission allows you to view the monitoring policies. The WRITE permission allows you to create and update monitoring policies. The DELETE permission allows you to delete monitoring policies.
	Performance Monitoring RESTCONF	Responsible for the retrieving the device performance metrics. The READ permission allows you to get the metrics information such as CPU, temperature, CRC, and interface utilization. The WRITE and DELETE permissions are not applicable for this API as there is no support for configuration-related operations.

Category	Global API Permissions	Description
Alarms and Events	Alarm Notification Policies	The READ permission allows you to read system/network, and device alarm notification policies. The WRITE permission allows you to create system/network, and device alarm notification policies.
	Alarm Settings	The READ permission allows you to view alarm settings. The WRITE permission allows you to view and update alarm settings.
	Alarm Suppression Policies	The READ permission allows you to view a suppression alarm policy. The WRITE permission allows you to create, update and delete a suppression alarm policy.
	Alarm & Events	Allows you to manage alarms. The READ permission allows you to get events/alarms according to request criteria, get the list of Syslog destinations, and get the list of trap destinations. The WRITE permission allows you to set a response for when an alarm is raised, acknowledged, or unacknowledged, create/raise an event, update the event info manifest, and add notes to alarms. The DELETE permission allows you to delete REST destinations, Syslog destinations and trap destinations.
	Alarm and Events RESTCONF	Responsible for performing alarms related operations. The READ permission allows you to get all the alarm data (system,network & device). The WRITE permission allows you to acknowledge, unacknowledge, and clear alarms. The DELETE permission is not applicable for these APIs.
Automated Assurance DSS Instance	Data Store Service Administrator Settings	Allows Administrators to view Datastore storage info (READ permission) and run diagnostic tests for external storage (WRITE permission).
	Data Store Service API	Allows you to use external storage for longer retention, and to manage external datastore used by Service Assurance for archiving service metrics data. The READ permission allows you to get storage provider information, check storage stats, etc. The WRITE permission allows you to sync the local CW datastore with the external storage and run diagnostics. The DELETE permission allows you to delete an external storage provider.

Category	Global API Permissions	Description
CNC	CAT FP Deployment Manager APIs	Allows you to manage function pack upload and deployment. The READ permission enables you to get the list of packages, files, and deployment information. The WRITE permission allows you to upload/deploy/un-deploy a package/function pack/file. The DELETE permission is not applicable for these APIs.
	CAT Inventory RESTCONF APIs	North Bound Interface (NBI) RESTCONF interface for the CAT services inventory data (from CAT to external consumers). The READ permission allows you to fetch the services information from CAT. The WRITE permission allows you to invoke operations APIs to retrieve the service information from CAT. The DELETE permission is not applicable for these APIs.
	CAT ISTP REST APIs	System use only. The READ/WRITE permissions are mandatory for CAT UI/ISTP to function. The DELETE permission is not applicable for these APIs.
	CAT Service Overlay	Primarily used to investigate issues in the overlay. Only READ permission is applicable.
	CAT UI	Mandatory APIs that enable CAT UI to fetch all NSO services and resources. The READ permission allows you to fetch and display all service information. The WRITE permission allows you to commit service assurance information. The DELETE permission is not applicable for these APIs.
	NSO Connector APIs	Allows you to perform services resync, full-resync, change log-level and return service HA status. The READ permission allows you to check the service status. The WRITE permission is required for all other operations. The DELETE permission is not applicable for these APIs.
	OAM Service APIs	Not Applicable

Category	Global API Permissions	Description
Change Automation	Administration APIs	Provides administrative control to manage job scheduling, manage override credentials, and configuration of user roles for playbook executions. The READ permission allows you to check the status and fetch the information. , while the WRITE permission allows you to make changes. The DELETE permission is not applicable for these APIs.
	Application APIs	Allows you to manage the Change Automation tasks (for example, schedule playbook executions, execute playbooks, update playbook jobs, check playbook executions status, check playbook job-set details, list supported YANG modules, etc.) The READ permission allows you to view the applicable information (for example, check the job status, fetch job details, etc.). The WRITE permission is required for playbook job scheduling/execution. The DELETE permission is not applicable for these APIs.
	Playbook APIs	Allows you to manage playbooks. The READ permission allows you to retrieve playbooks, params, and policy specs. The WRITE permission allows you to import/export, and generate playbooks. The DELETE permission enables you to delete playbooks.
	Play APIs	Allows you to manage plays. The READ permission allows you to fetch or view plays, while the WRITE permission allows you to create, update or import a play. The DELETE permission allows you to delete a play.

Category	Global API Permissions	Description
Collection Infra	Collection APIs	Permissions for APIs to manage collection jobs. Based on the READ/WRITE/DELETE permissions, you can view collection jobs, create/update new collection jobs (external), or delete existing collection jobs. System collection jobs (data collection setup internally for Crosswork consumption) cannot be modified irrespective of these permissions (permitted for Administrators only), but users with the READ permission will be able to view the details of all collection jobs including system collection jobs. For most users, READ-only permissions would be enough as it enables them to view Collection jobs detail (request and status) and actual data collection status/metrics per device/sensor path level.
	Data Gateway Manager APIs	Permissions to perform CRUD operations on Destinations, Data Gateways, Custom Packages, etc. The READ permission allows you to view the data, while the WRITE permission allows you to perform these actions: • Add, edit, or delete Data Gateways and Data Gateway instances. • View the vitals • Add, edit, delete, and view the custom packages • View the system packages • Add, edit, or delete data destinations • Update resources • Create, edit, or delete Data Gateway pools • Revoke the provisioning permission from task permissions • Restrict user access by revoking the Inventory API, Data gateway APIs, and Platform APIs permissions. • Troubleshoot data collection issues

Category	Global API Permissions	Description
Crosswork Optimization Engine	OPTIMA Analytics	Allows you to manage analytics in Crosswork Optimization Engine. The READ permission allows you to view/export historical data. The WRITE permission enables you to change the Traffic Engineering Dashboard settings. The DELETE permission is not applicable for these APIs.
	OPTIMA Analytics Service	Allows you to manage analytics service in Crosswork Optimization Engine. The READ permission enables you to get LSP events data, LSP utilization, LSP SR-PM metric, Link SR-PM and underutilized LSPs. The WRITE and DELETE permissions are not applicable for these APIs.
	Optima Engine RESTCONF and Optima Engine RESTCONF API for backwards compatibility	

Category	Global API Permissions	Description
		Allows you to customize the RESTCONF API permissions in Crosswork Optimization Engine. The READ permission grants access to perform these actions: • Fetch L2 and L3 topology details, as well as Segment Routing policy information • Preview SR Policy route • Filter SR Policies on Interfaces and nodes • Preview RSVP-TE tunnels • Get LCM domains and LCM recommendation SR Policies • Preview LCM recommendations • Get LCM configuration and managed interfaces • Get Circuit Style SR Policy paths on interfaces and nodes • Get all Circuit Style SR Policy paths • Get Circuit Style Manager interface bandwidth pool • Get a plan file for the network model The WRITE permission grants access to perform these actions: • Provision, modify, and delete SR policies • Provision, modify, and delete RSVP-TE tunnels • Provision, modify, and delete SR P2MP policies • Configure LCM configuration and managed interfaces • Remove LCM domains • Commit and pause LCM recommendations • Set CSM interface bandwidth pool • Create notification streams • Reoptimize Circuit Style SR policies The DELETE permission is not applicable for these APIs.
	Optimization Engine UI	

Category	Global API Permissions	Description
		Allows you to manage SR policies, RSVP tunnels, LCM, BWoPT, BWoD, Traffic Engineering settings, and Preview policies. The READ permission allows you to view deployed policies, settings, routes, LCM domain config/data, service overlay data, path queries, dashboard metrics, etc. The WRITE permission allows you to configure LCM, BWoD, BWopt, deploy policies, preview Crosswork Optimization Engine-managed policies, etc. The DELETE permission allows you to delete SR policies, RSVP tunnels, remove affinity mapping, and delete LCM domains.
Crosswork Optimization Engine v2	Optimization Engine RESTCONF API v2	Allows you to customize the RESTCONF interface permissions in Crosswork Optimization Engine. The READ permission enables you to fetch L2 and L3 topology details, and Segment Routing Policy details. The WRITE permission allows you to fetch policy routes, provision/modify/delete/preview SR policies, and manage LCM configuration. The DELETE permission is not applicable for these APIs.
Data Gateway Global Settings	Data Gateway Global Parameters API	There are certain parameters in the data gateway, which can be changed globally across all gateways in a Deployment. The READ permission allows you to view the data, while the WRITE permission is required to reset/update the data.
	Data Gateway Global Resources Reset API	Allows you to reset updates done to the Global Parameters. The READ permission allows you to view the data, while the WRITE permission resets the data.
	Data Gateway Global Resources Update API	Allows you to update the Global Parameters. The READ permission allows you to view the data, while the WRITE permission updates the data.
Data Gateway Troubleshooting	Data Gateway Reboot API	Reboots a data gateway. The WRITE permission allows you to reboot the data gateway.
	Data Gateway Showtech API	Generates and downloads showtech logs for a data gateway. The READ permission allows you to view showtech, while WRITE permission generates showtech. Write Permission allows u to generate showtech

Category	Global API Permissions	Description
Health Insights	Health Insights APIs	Allows you to manage Health Insights KPIs. The READ permission allows you to view all KPIs, KPI profiles, job details, alerts, etc. The WRITE permission allows you to create or update KPIs and KPI profiles, enable/disable KPI profiles, link KPIs to playbooks, etc. The DELETE permission allows you to delete custom KPIs and KPI profiles.
Inventory	Inventory APIs	Allows you to manage inventory. The READ permission allows you to • Fetch the list of nodes, the node credentials, and the count of nodes in the database. • Retrieve the list of HA pools, data gateway enrollments, virtual data gateways, and inventory job information. • Retrieve the list of policies, providers, and tags. The WRITE permission allows you to • Update device mapping to virtual data gateway pool. • Lock/unlock the requested nodes. • Remove tag associations from nodes. Does not support partial un-assignment. • Update input data to a set of devices. • Set API endpoint for provider onboarding. • Update collections job cadence The DELETE permission allows you to • Perform bulk deletion of credential profiles and nodes. • Upload CSV for delete operations. • Delete HA pools, Data Gateway enrollments, and virtual data gateways. • Delete policies, providers, and tags.

Category	Global API Permissions	Description
Platform	Platform APIs	The READ permission allows you to fetch the server status, cluster node information, application health status, collection job status, certificate information, backup and restore job status, etc. The WRITE permission allows you to • Enable/disable the maintenance mode • Enable/disable the xFTP server • Manage cluster (set the login banner, restart a microservice, etc.) • Rebalance cluster resources • Manage nodes (export cluster inventory, add VM, apply VM configuration, remove VM from a cluster, etc.) • Manage certificates (export trust store and intermediate key store, create or update certificate, configure the web server, etc.) • Perform normal/data-only backup and restore operations. • Manage applications (activate, deactivate, uninstall, add package, etc.) The DELETE permission allows you to delete a VM (identified by an ID) and remove applications from the software repository.
	Grouping APIs	Grouping management and Topology groups selection tree. The READ permission allows you to view topology UI, while the WRITE permission allows you to create/update groups. The DELETE permission is needed to delete groups from the Grouping Management page. **Note** When READ access is removed for Grouping APIs, in addition to being blocked out of the Grouping window, the users will also be unable to access the Traffic Engineering, VPN Services, and Topology Services windows.
	View APIs	Views Management in Topology. The READ permission allows you to see views, the WRITE permission allows you to create/update views, and the DELETE permission will enable delete capabilities.

Category	Global API Permissions	Description
Topology	Geo	Provides geo service for offline maps. The READ permission allows you to use Geo Map in offline mode, the WRITE allows you to upload Geo Map files, and DELETE permission allows you to delete the map files in settings.
	Topology	Allows you to manage topology pages, settings, or any other pages that uses the Topology visualization framework. The READ permission is mandatory for topology visualization. The WRITE permission enables you to update topology settings, and the DELETE permission allows you to delete a topological link if it goes down.
Probe Manager	Probe Manager APIs	The READ permission allows you to retrieve the status of a probe session for a given service. The WRITE permission allows you to reactivate a probe. The DELETE permission is not applicable for these APIs.
Proxy	Crosswork Proxy APIs	Permissions to manages Crosswork proxy APIs for NSO Restconf NBI. The READ permission allows all GET request for NSO REST conf NBI, the WRITE permission allows POST/PUT/PATCH operation, and the DELETE permission enables all delete APIs.
Software Image Management	SWIM	Allows you to upload images to the SWIM repository, distribute them to devices and install them. The READ permission allows you to list all images from the SWIM repository, view image information from a device, and check the details of any SWIM job. The WRITE permission allows you to upload/distribute and perform all install-related operations. The DELETE permission allows you to delete copied images from a device. You require WRITE/DELETE permission to execute software install/uninstall playbooks in Change Automation.

Category	Global API Permissions	Description
Service Health	Archiver APIs	The READ permission allows you to • Check if Historical Data exists for a given service. • Get the Historical Timeline series for a given service. • Get a Service Graph for a selected timestamp of the service. • Retrieve probe and 24 hours metric data for a given service. The WRITE/DELETE permissions are not applicable for these APIs.
	Assurance Graph Manager APIs	The READ permission allows you to: • Fetch details of a service. • Get the impacted list of services. • Retrieve the list of matching sub-services (transport or device only). The WRITE/DELETE permissions are not applicable for these APIs.
	CAT SH UI	The READ permission allows you to: • Retrieve service data, including the total number of monitored services, the count of basic services, and the count of advanced services. • Retrieve the number of services based on health status (for example, Good, Degraded, Down, Error, Initiated, and Paused). • Retrieve the number of provisioned and monitored services categorized by service type (L2 and L3). The WRITE/DELETE permissions are not applicable for these API.
	Config Manager APIs	The READ permission allows you to: • Retrieve advanced and total counts of services with monitoring enabled and published. • Force reconciliation with ISTP. The WRITE permission allows you to update the maximum number of services supported for Total and Advanced monitoring. The DELETE permission is not applicable for these APIs.
	Heuristic Package Manager APIs	

Category	Global API Permissions	Description
		Permissions for Heuristic package management and to manage plugins and config profiles for Service Assurance. The READ permission allows you to export heuristic packages, query for heuristic package details (Rules, Profiles, SubServices, Metrics, Plugins), and query for assurance options. The WRITE permission allows you to import heuristic packages and perform all create/update operations. The DELETE permission allows you to perform delete operations (for example, delete the RuleClass, MetricClass, etc.)
	Metric Scheduler APIs	Not Applicable

Category	Global API Permissions	Description
Zero Touch Provisioning	Config Service	The READ permission allows you to • List all day-0 configuration files stored in the ZTP config repository. • Fetch count of day-0 configuration files stored in the ZTP config repository. • Download the day-0 configuration file from the ZTP config repository. • List all device family/device versions and device platforms based on information associated with day-0 config files stored in the CW ZTP repository. The WRITE permission allows you to • Upload the day-0 config file or script to the ZTP config repository. • List/update relevant metadata associated with specific day-0 config files stored in the ZTP config repository The DELETE permission allows you to delete config files and scripts uploaded in the ZTP config repository.
	Image Service	The READ permission allows you to • List all device image files stored in the ZTP image repository. • List all device platform/family names associated with image files stored in the CW ZTP repository. • Download the device image file by ID. The WRITE permission allows you to update relevant metadata associated with specific image files stored in the ZTP image repository. The DELETE permission allows you to delete image files uploaded in the ZTP image repository
	ZTP Service	Allows you to manage the ZTP devices and profiles - add/update/delete into Crosswork. The READ permission enables you to fetch ZTP devices, serial number/OVs, profiles, sample data CSV, list ZTP devices, profiles, and export ZTP devices and metadata. The WRITE permission allows you to add ZTP devices, serial numbers/OVs, profiles and add/update the ZTP device's attributes. The DELETE permission allows you to delete ZTP devices, profiles, serial numbers/ownership vouchers.

Category	Global API Permissions	Description
Licensing	Common Licensing Management Service (CLMS) APIs	Permissions for APIs to manage license registration in Crosswork. The READ permission enables you to view Smart Licensing settings, registration status, and license usage while the WRITE permission is required to change any Smart Licensing setting such as register, re-register, de-register, renew a license etc. The DELETE permission is not applicable for these APIs.
te-manager	TE Auto Policy Binding Service	The READ permission allows you to view individual or all TE criteria and policy templates. The WRITE permission allows you to create or update TE criteria, criteria expression, and policy templates, and to associate or disassociate TE criteria with policy templates and vice versa. The DELETE permission allows you to delete TE criteria, criteria expression, and policy templates, and remove any residual data associated with a service.

Manage Active Sessions

As an administrator, you can monitor and manage the active sessions in the Cisco Crosswork UI, and perform the following actions:

- Terminate a user session
- View user audit log

Attention

- Non-admin users with permission to terminate can terminate their own sessions.
- Non-admin users with read-only permission can only collect the audit log for their sessions.
- Non-admin users without read permissions can't view the **Active Sessions** window.

Procedure

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

The **Active Sessions** tab displays all the active sessions in the Cisco Crosswork with details such as user name, source IP, login time, and login method.

Note
The **Source IP** column appears only when you check the **Enable source IP for auditing** check box and relogin to Cisco Crosswork. This option is available in the **Source IP** section of the **Administration** > **AAA** > **Settings** page.

Step 2 To terminate a user session, click the  icon under the **Actions** column, and select **Terminate Session**. A dialog box is displayed to confirm your action. Select **Terminate** to terminate the session.

Attention

- You are recommended to use caution while terminating a session. A user whose session is terminated will not receive any prior warning and will lose any unsaved work.
- Any user whose session is terminated will see the following error message: `"Your session has ended. Log into the system again to continue"`.

Step 3 To view audit log for a user, click the  icon under the **Actions** column, and select **Audit Log**.

The **Audit Log** window is displayed for the selected user name. For more information on the Audit Logs, see View Audit Log, on page 475.

Manage WebSocket subscriptions

If you have subscribed to WebSocket subscriptions using **JWT** based authentication to authenticate and establish your connections, you can view these subscriptions in the Crosswork Network Controller UI. The types of subscriptions that are supported are:

- Inventory
- Alarm
- Service Notification

Procedure

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

Step 2 Click **WebSocket subscriptions**.

It displays details such as **Subscription ID**, **Topic**, **Subscribed By**, **Subscription Time** and **Source IP.**

Note

- The **Source IP** column appears when you check the **Enable source IP for auditing** check box. This option is available in the Source IP section of the **Administration** > **AAA** > **Settings** page.

Step 3 To delete a subscription, choose the subscription you want to remove and click the **Delete** icon.

Manage Device Access Groups

Crosswork offers access control based on user roles, with read/write/delete permissions for specific APIs grouped by functional areas.

While this centralizes access control, it does not extend to device-level access. To manage device access for users, Device Access Groups can be used to logically group devices. Non-admin users assigned to the system-level task of Device Access Groups management can create and manage these groups.

APIs, Tasks and Device Access Groups- Know the Difference

Device Access Groups are not directly related to API access control or task-based access control. Here's a breakdown of their differences and roles:

- **APIs**: Control read/write/delete access levels to the APIs but do not control the UI access of a user. Permissions for APIs are defined and enforced at the API level, allowing administrators to specify what actions a user can perform.
- **Tasks**: Control access to certain functionalities by combining a set of APIs. Enabling a specific task also enables the corresponding APIs required for that task.
- **Device Access Groups**: Serve as an extra security layer to control access to specific devices or resources within Crosswork, beyond API and task-based access controls. They are used to logically group devices for user management.

Administrators have full control over building user roles and permissions, including defining Device Access Groups. Device Access Groups become relevant only after a user has passed the initial API-based and/or task-based access controls set by an administrator. Once these initial access levels are granted, Device Access Groups provide additional control over which devices a user can have WRITE permissions for provisioning.

Administrators can configure Device Access Groups according to specific requirements, adding an extra layer of control and customization for access management within Crosswork.

How do Device Access Groups work?

When a user is associated with one or more Device Access Groups, they can make configuration changes and provision services on the devices within those groups. A Crosswork user with an administrator role or a mapped Device Access Groups management task can:

- Create and manage Device Access Groups.
- Assign users to specific Device Access Groups.
- Define and control which devices users can access and modify.
- Ensure that users have the appropriate permissions to perform their tasks on designated devices.

Important Device Access Groups control device-level WRITE or Provisioning and Crosswork flows that trigger such operations. They do not affect WRITE or EDIT operations within Crosswork itself.

You can restrict users to specific tasks based on their role's permissions, ensuring only authorized individuals have access and control over their actions within the system. Crosswork's role-based access control synchronizes

with NSO and Device Access Groups to streamline device configurations, using JWT tokens for authentication and authorization in RESTCONF and JSON-RPC API workflows. However, reverse synchronization is not possible; changes in NSO are not reflected in Crosswork Device Access Groups (for detailed information on the prerquisites for setting up NSO, see Configure NSO Servers, on page 418). External LDAP, TACACS, and RADIUS servers support Device Access Groups integration.

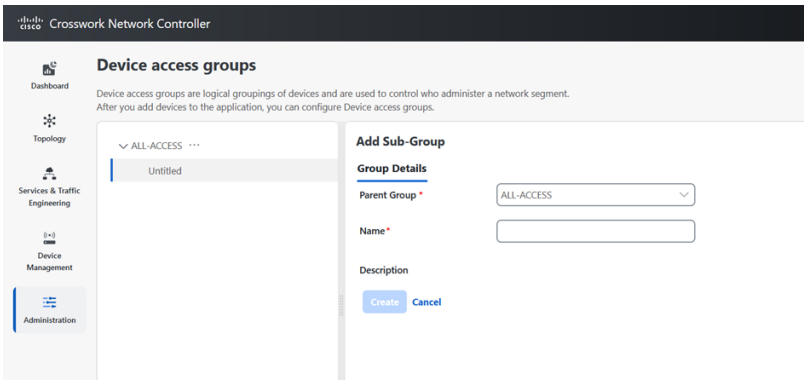
Create Device Access Groups

To enable seamless device-level granular Role-Based Access Control across Crosswork applications and integrated NSO, create a Device Access Group that will allow for centralized management of device access permissions, ensuring consistent role based access implementation across the system. Only users belonging to a role that has the "Device Access Group Management" task enabled have the ability to perform Create, Read, Update and Delete operations on the Device Access Groups.

Procedure

Step 1 From the main menu, choose **Administration** > **Device Access Groups**.

Step 2 Click the icon next to ALL-ACCESS, then click **Add Sub-Group.**



Step 3 Add the name and description of the sub-group under **Group Details**.

Step 4 Click **Create.**

When you add a devices to a Device Access Group, you can view the **Devices** tab next to **Group Details**.

Step 5 Click on **Add Devices**.

Step 6 Select the devices you want to add and click **Save**.

You can also filter the devices that you want to add using the **Filter By** options for **Host Name, Product Type and Node IP**. The devices are added under Device Access Groups as well as updated in the NSO site.

Step 7 Click **Save**.

Edit Device Access Groups

You can add or remove a device from an existing Device Access Group.

Attention The delete group check is only relevant for local users defined in Crosswork and does not apply to users managed by external AAA servers.

Procedure

Step 1 From the main menu, choose **Administration** > **Device Access Groups**.

Step 2 Click the Device Access Group that you want to edit and then click **Edit Group**.

You can add more devices by clicking **Add Devices** or remove them by clicking **Remove Devices**.

Step 3 Click **Save**.

Note
You cannot delete a Device Access Group if a user is exclusively associated with it. However, if all users associated with the Device Access Group also belong to other Device Access Groups, you can delete it.

Assign Task permissions

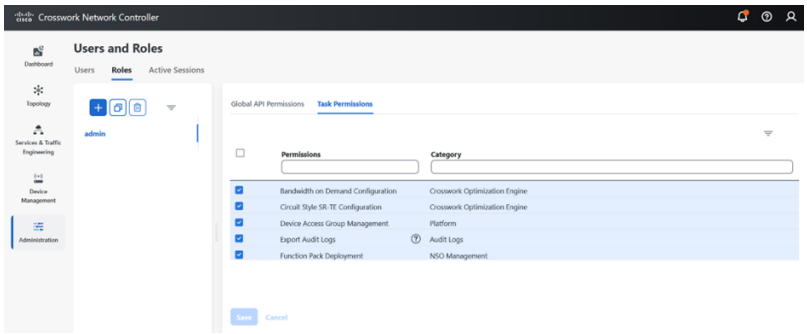
You can assign the tasks that you have created to a specific role. You can enable or disable these tasks based on the permissions you want to give for a role. The task permissions are defined by the Global APIs, which allow you to assign **Read/Write/Delete** permissions for that specific task.

Procedure

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

Step 2 Click **Task Permissions** to view a list of all the available tasks for your application.

Figure 84: Users and Roles Window



Step 3 Select the task for which you want to assign permissions. Under the **Global API Permissions** tab, you can also view the specific **Read/Write/Delete** permissions that are automatically enabled for the selected task.

Step 4 Click **Save**.

Associate a User with a Device Access Group

Once you have created a user, you can associate that user with a specific Device Access Group. You can then assign task permissions for this user, which lets you restrict or allow certain tasks for them.

Procedure

Step 1 Create a role with **read/ write/ delete** API permissions and assign the set of specific tasks that need to be enabled within each role. Refer to the section, User Roles, Functional Categories and Permissions, on page 393 for more details.

Step 2 Assign this role and one or more Device Access Group to a user. Refer to the section, Manage Users, on page 391 for more details.

When the user logs in, the user can only perform operations allowed by the tasks on devices belonging to the associated Device Access Groups. Based on task permissions and Device Access Group privileges, a restricted read-only Device Access Group user has the following capabilities while provisioning policies on BWoD, LCM, CSM, DLM, DGM and CAT. Such a user can-

- Preview and dry run policies but cannot provision or commit changes for the policies.
- View Services and Traffic Engineering configuration pages but cannot edit or import files.
- Perform Path Query operations.
- View Services and Traffic Engineering configuration pages but cannot edit or import files.
- Create VPN services.
- View the devices that are associated with a failed service, along with the detailed error message but cannot take actions on the errors.

Correspondingly, a Device Access Group user with all the **read/ write/ delete** permissions has the following capabilities. Such a user can-

- Perform all the tasks listed for a restricted read-only Device Access Group user.
- Provision policies for which they have been granted access to. For instance, if a user wants to create an RSVP-TE policy on a Tunnel, they will be able to do so only if they have been granted access to the head-end node. However, note that access to the end-points and hops is not checked for Device Access Group control.
- View the devices that are associated with a failed service, along with the detailed error message. Additionally, users with all privileges can take actions on errors such as Check-Sync, Sync-To, and Compare-Config at the node level.
- Run and execute Playbooks.

Note
To restrict device access in Crosswork for read-only users, the administrators must create an empty Device Access Group (for example, NO_DEVICE_ACCESS) without any devices, and assign it while creating read-only user profiles (or user profiles associated with read-only roles).

Configure NSO Servers

The integration of authentication and authorization between Crosswork and NSO for RESTCONF and JSON-RPC API workflows is facilitated through the use of JWT. To enable role-based access control and seamless synchronization between Crosswork and NSO refer to the prerequisite steps listed under the following sections:

- Configure Standalone NSO, on page 418
- Configure LSA NSO, on page 423

Note

- Only administrators are allowed to make modifications to tasks.
- If any changes are made to NACM settings, the user must log out and then log back in. This is necessary to regenerate the JWT.
- When a user with limited device access tries to edit a service or upload an XML file in the Provisioning UI, the **commit** button is enabled. However, it throws an error when the user clicks the **commit** button.

Configure Standalone NSO

Follow the steps below to configure a standalone NSO server to sync role-based access control functions with Crosswork.

Procedure

Step 1 Enable `cisco-cfp-jwt-auth`.

a) **Update the ncs.conf file:** Open the `ncs.conf`` file in the NSO directory. Add the following configuration under the <aaa> section.

```
 <aaa>
    <package-authentication>
     <enabled>true</enabled>
     <packages>
       <package>cisco-cfp-jwt-auth</package>
     </packages>
    </package-authentication>
</aaa>
- Make sure to restart ncs for the configuration in ncs.conf to take effect:
   /etc/init.d/ncs restart
```

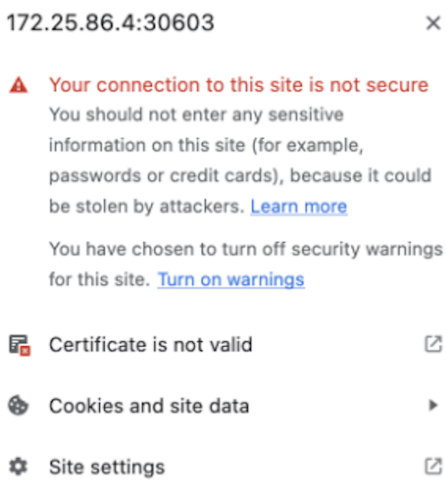
Note
Make sure to restart NCS for the configuration in the `ncs.conf` file to take effect. If you do not want to use this feature, change 'package-authentication' to 'false' in `'ncs.conf` in the AAA section under the NCS configuration file and restart NCS. This disables the package authentication for `'cisco-cfp-jwt-auth'`.

b) Copy the certificate file from Crosswork to the NSO VM. To get the certificate from Crosswork to NSO VM, follow these steps:

1. Open the Chrome browser and navigate to the Crosswork website for which you want to import the certificate.

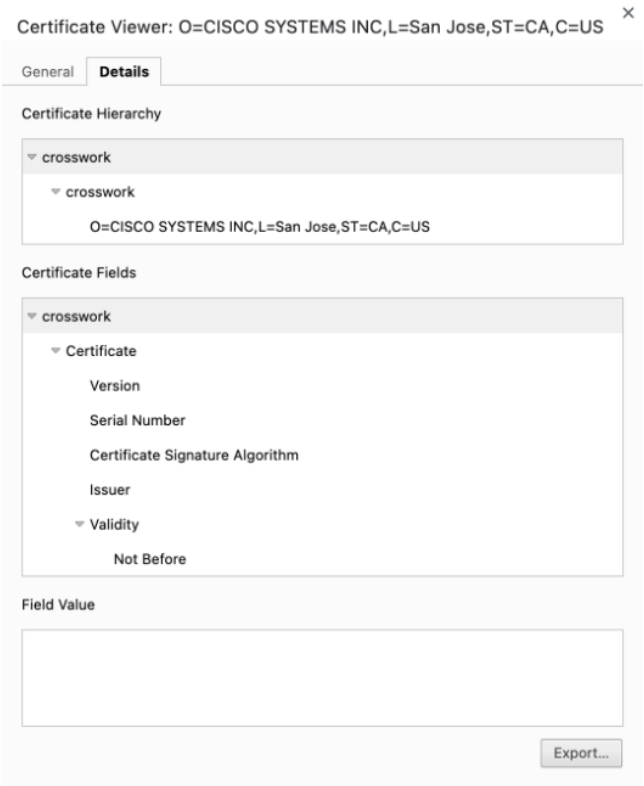
2. Click the padlock icon in the address bar to view the site information and then click **Certificate is not Valid** > **View Certificate**.

Figure 85: View Certificate Window



3. In the **Certificate Viewer** window, go to the **Details** tab.

Figure 86: Details for Certificate Viewer

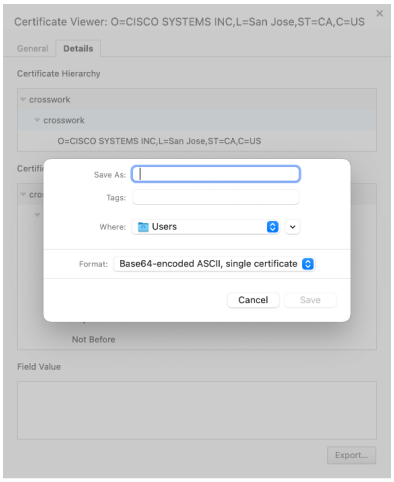


4. Click **Crosswork** under **Certificate Hierarchy**.

5. Click the **Export** button and choose a file name and location to save the certificate. Choose the **Base64-encoded ASCII, single certificate** option and save it with the extrension **.pem**. For example: crosswork.pem.

   Note
   In case you encounter issues saving the file in the .pem format, an alternative is to save it as a .cer file. Once saved, proceed to use this .cer file during the bootstrap configuration process. Make sure to reference the file path of the .cer file in all subsequent steps that require it.

   Figure 87: Save the Certificate Window



6. Copy the .**pem** file to NSO VM.

   Note
   Make sure that the value of the **pem-key-path** parameter and the filename are the same on the primary and secondary host.

c) **Configure Bootstrap:** To configure the Bootstrap authentication package, perform the following steps:

   Login to NSO VM and load the cw-jwt-auth.xml file using the **merge** operation.

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <jwt-auth xmlns="http://cisco.com/ns/nso/cfp/cisco-cfp-jwt-auth">
    <ip-address>172.20.100.42</ip-address>
    <port>30603</port>
    <pem-key-path>/home/nso/crosswork.pem</pem-key-path>
  </jwt-auth>
</config>
```

   OR

   Log in to `ncs_cli` and enter config mode.

```
set jwt-auth cnc-host <Crosswork IP>
set jwt-auth port 30603
set jwt-auth pem-key-path /home/nso/crosswork.pem
commit
```

Step 2 Enable service level NACM.

Before creating a Rule-list, create the NACM group manually and update the user as needed when the same group applies to more that one user.

```
ncs_cli -u admin
configure
set nacm enforce-nacm-on-service true
commit dry-run
commit
```

Step 3 Create NACM Groups and Rule list.

a) **For admin users:** Follow the steps below to create NACM groups and Rule-list for admin users.

1. **User Association:** If a NSO user is an admin user, they will automatically be part of the "ncsadmin" group, which grants them all access by default. However, if the admin user does not add this user to the "CNC#ALL-ACCESS" group, the functionalities will still work properly. If the NSO user has a different name, such as "cisco", then you must add the user to the "CNC#ALL-ACCESS" group.

   Note that user creation is not required at this point.

2. **Create Device group:** When a Device Access Group gets created in Crosswork, an equivalent device-group is created in NSO.

   Note that the ALL-ACCESS Device Access Group is not created by default, and is not needed for an admin user. If you want, you can create it manually using the following command, where **group-name** is the name of the group you create.

   ```
   ncs_cli -u admin
   configure
   set devices device-group "group-name" device-name [ device-host-name1, device-host-name2]
   commit dry-run
   commit
   ```

   You can also copy this from Crosswork by navigating to **Administration** > **Users and Roles** > **Users** > **Generate NACM Rules**.

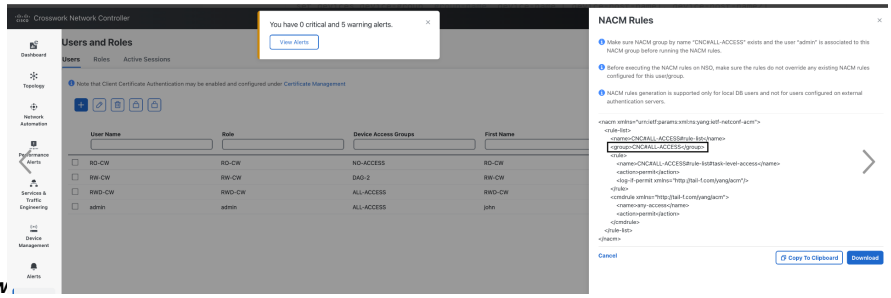


Figure 88: Generate NACM Rules Window

3. Create a NACM group manually and update the user as needed when the same group applies to more that one user. Make sure to do this before you create the Rule-list.

   ```
   ncs_cli -u admin
   configure
   set nacm groups group "CNC#ALL-ACCESS" user-name admin
   commit dry-run
   commit
   ```

4. **Create NACM Rule list:** When a User with a Role and Device Access Group is set in Crosswork, the UI displays an option to generate the NACM rules under each user. You can either copy these rules and apply them to NSO using the **commit manager** or copy the xml to the file <sample-nacm.xml> and load it using the **merge** operation. Note that for admin users only the task level access and cmd-rule are required.

   ```
   <nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
       <rule-list>
   ```

```
        <name>CNC#ALL-ACCESS#rule-list</name>
        <group>CNC#ALL-ACCESS</group>
        <rule>
            <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <cmdrule xmlns="http://tail-f.com/yang/acm">
            <name>any-access</name>
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
```

b) **For non-admin users:** Follow the steps below to create NACM groups and Rule-list for non- admin users.

In the code sample below, we have used RW-CW as an example for non-admin user and DAG-2 as a Device Access Group name.

1. **Create NACM Group:** See the code sample below:

```
ncs_cli -u admin
configure
set nacm groups group "CNC#DAG-2" user-name RW-CW
commit dry-run
commit
```

You can copy the Group name from Crosswork using the **Generate NACM Rules** option.

2. **Create NACM Rule list:**You can copy the Rule list from Crosswork using **Generate NACM Rules** option. Here is a sample-

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <rule-list>
        <name>CNC#DAG-2#rule-list</name>
        <group>CNC#DAG-2</group>
        <rule>
            <name>CNC#DAG-2#rule-list#allow-DAG-2</name>
            <device-group
xmlns="http://tail-f.com/yang/ncs-acm/device-group-authorization">DAG-2</device-group>
            <access-operations>create read update delete exec</access-operations>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <rule>
            <name>CNC#DAG-2#rule-list#deny-others</name>
            <path>/devices</path>
            <access-operations>create update delete exec</access-operations>
            <action>deny</action>
        </rule>
        <rule>
            <name>CNC#DAG-2#rule-list#task-level-access</name>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <cmdrule xmlns="http://tail-f.com/yang/acm">
            <name>any-access</name>
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
```

You can push these rules to NSO via commit manager or copy them to a xml file (For example: sample-nacm.xml) and then add it on NSO with these commands:

Load sample-nacm.xml

```
ncs_cli -u admin
configure
load merge /home/nso/sample-nacm.xml
commit
```

Configure LSA NSO

Follow the steps below to configure a LSA NSO server to sync role-based access control functions with Crosswork.

Procedure

Step 1 Enable local authentication in the `ncs.conf` file under the AAA section on all the NSO RFS nodes. (If you are using the CFS node, you can skip this step)

```
<local-authentication>
      <enabled>true</enabled>
</local-authentication>
```

Restart NSO by running the command `sudo /etc/init.d/ncs restart` on each RFS node.

Step 2 **Enable cisco-cfp-jwt-auth:** Refer to the same steps to enable `cisco-cfp-jwt-auth` as described in the section, Configure Standalone NSO, on page 418.

Make sure that the value of the **pem-key-path** parameter and the filename are the same on the primary and secondary host.

Step 3 Enable service level NACM.

```
ncs_cli -u admin
configure
set nacm enforce-nacm-on-service true
commit dry-run
commit
```

You must enable this on both the CFS and RFS nodes.

Step 4 Create NACM Groups and Rule list. (This is applicable for both admin users and non admin-users)

a) **Associate Users:** To enhance security with LSA role-based authentication in NSO, we recommend that you remove the "auth-group default" map if NSO is exclusively used with Crosswork. However, if there are non-Crosswork NSO users, they must use the default map. In this case, every Crosswork user must have an entry in the "auth-group umap" to ensure the Role-Based Access Control flow functions correctly.

b) Define a Crosswork user under "aaa:aaa" as an authentication user on every RFS node. This configuration enables communication between CFS and RFS for this user. Note that the username must match the username used in Crosswork, but the password can differ.

c) Add every Crosswork user as a "umap" entry under the device authentication group in the CFS. This ensures proper functionality and enforces Role-Based Access Control for users in Crosswork. This also allows the CFS to pass user requests to the RFS node as the corresponding user. If you want a role-based access for a user, you must create the umap entry in the CFS auth-group. Otherwise, the default map applies, which breaks the role-based access workflow.

d) Define a generic NACM group and NACM rule with all permissions on the CFS, to enable access to RFS nodes for all users. This grants access to RFS for all users. Additionally, when creating any user in Crosswork, add that user to the "CNC#ALL-ACCESS" NACM group in CFS. This ensures that the user has the necessary access privileges and permissions to perform actions within Crosswork.

```
group "CNC#ALL-ACCESS" {
        user-name [ RW-CW admin rw-user ];
    }
```

You can copy the NACM rules from Crosswork.

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <!--NACM rules for NSO - CFS-->
    <rule-list>
        <name>CNC#ALL-ACCESS#rule-list</name>
        <group>CNC#ALL-ACCESS</group>
        <rule>
            <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <cmdrule xmlns="http://tail-f.com/yang/acm">
            <name>any-access</name>
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <!--NACM rules for NSO - RFS-->
    <rule-list>
        <name>CNC#ALL-ACCESS#rule-list</name>
        <group>CNC#ALL-ACCESS</group>
        <rule>
            <name>CNC#ALL-ACCESS#rule-list#task-level-access</name>
            <action>permit</action>
            <log-if-permit xmlns="http://tail-f.com/yang/acm"/>
        </rule>
        <cmdrule xmlns="http://tail-f.com/yang/acm">
            <name>any-access</name>
            <action>permit</action>
        </cmdrule>
    </rule-list>
</nacm>
```

Step 5 **Create Device group:** Add the Device Access Groups and NACM rules on the RFS node. By defining NACM rules for a user, access to devices can be granted based on the specific rules that you configure for that user. Note that Device Access Group creation is automatically handled by Crosswork, so you do not need any additional steps for Device Access Group creation on NSO.

Note
If you have Geo-HA set up, and encounter the 503 error, follow the steps below to resolve it.

Add the following configurations exclusively to the **/etc/environment** file within the CFS node:

a) Open the file `sudo vi /etc/environment`.
b) Add the following lines:

```
https_proxy="http://proxy.esl.cisco.com:80"
http_proxy="http://proxy.esl.cisco.com:80"
```

c) Define exceptions with the line:

```
no_proxy="localhost,127.0.0.1,10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,cisco.com,<az1 mgmt vip>,<az2
 mgmt vip>,<fqdn of CW geo-mgmt VIP>"
```

For example:

```
no_proxy="localhost,127.0.0.1,10.0.0.0/8,192.168.0.0/16,172.16.0.0/12,cisco.com,
192.168.6.50,192.168.5.50,geomanagement.cw.cisco,cw.cisco"
```

d) Source the file: `source /etc/environment`
e) Reboot the CFS nodes for the proxy settings to take effect.

Security Hardening Overview

Security hardening entails making adjustments to ensure that the following components optimize their security mechanisms:

- Cisco Crosswork infrastructure
- Cisco Crosswork storage system (local or external)

Hardening Cisco Crosswork security requires completion of the following tasks:

- Shutting down insecure and unused ports
- Configuring network firewalls
- Hardening the Cisco Crosswork infrastructure, as needed

Although your primary source of information is your Cisco representative, who can provide server hardening guidance specific to your deployment, you can also follow the steps in this section to secure Cisco Crosswork.

Authentication Throttling

Cisco Crosswork throttles the login attempts after a failed login attempt to avoid password guessing and other related abuse scenarios. After a failed login attempt for a username, all authentication attempts for that username would be blocked for 3 seconds. The throttling is applicable to all supported authentication schemes such as TACACS, LDAP and the default local authentication.

Core Security Concepts

If you are an administrator and are looking to optimize the security of your Cisco Crosswork product, you should have a good understanding of the following security concepts.

HTTPS

Hypertext Transfer Protocol Secure (HTTPS) uses Secure Sockets Layer (SSL) or its subsequent standardization, Transport Layer Security (TLS), to encrypt the data transmitted over a channel. Several vulnerabilities have been found in SSL, so Cisco Crosswork now supports TLS only.

Note TLS is loosely referred to as SSL often, so we will also follow this convention.

SSL employs a mix of privacy, authentication, and data integrity to secure the transmission of data between a client and a server. To enable these security mechanisms, SSL relies upon certificates, private-public key exchange pairs, and Diffie-Hellman key agreement parameters.

X.509 Certificates

X.509 certificates and private-public key pairs are a form of digital identification for user authentication and the verification of a communication partner's identity. Certificate Authorities (CAs), such as VeriSign and Thawte, issue certificates to identify an entity (either a server or a client). A client or server certificate includes the name of the issuing authority and digital signature, the serial number, the name of the client or server that the certificate was issued for, the public key, and the certificate's expiration date. A CA uses one or more signing certificates to create SSL certificates. Each signing certificate has a matching private key that is used to create the CA signature. The CA makes signed certificates (with the public key embedded) readily available, enabling anyone to use them to verify that an SSL certificate was actually signed by a specific CA.

In general, setting up certificates in both High Availability (HA) and non-HA environments involves the following steps:

1. Generating an identity certificate for a server.
2. Installing the identity certificate on the server.
3. Installing the corresponding root certificate on your client or browser.

The specific tasks you need to complete will vary depending on your environment.

Note the following:

- The start-stop sequencing of servers needs to be done carefully in HA environments.
- Non-HA environments, where a virtual IP address is configured, require the completion of a more complicated certificate request process.

1-Way SSL Authentication

This authentication method is used when a client needs assurance that it is connecting to the right server (and not an intermediary server), making it suitable for public resources like online banking websites. Authentication begins when a client requests access to a resource on a server. The server on which the resource resides then sends its server certificate (also known as an SSL or x.509 certificate) to the client in order to verify its identity. The client then verifies the server certificate against another trusted object: a server root certificate, which must be installed on the client or browser. After the server has been verified, an encrypted (and therefore secure) communication channel is established. At this point, the Cisco Crosswork server prompts for the entry of a valid username and password in an HTML form. Entering user credentials after an SSL connection is established protects them from being intercepted by an unauthorized party. Finally, after the username and password have been accepted, access is granted to the resource residing on the server.

Note A client might need to store multiple server certificates to enable interaction with multiple servers.

To determine whether you need to install a root certificate on your client, look for a lock icon in your browser's URL field. If you see this icon, this generally indicates that the necessary root certificate has already been installed. This is usually the case for server certificates signed by one of the bigger Certifying Authorities (CAs), because root certificates from these CAs are included with popular browsers.

If your client does not recognize the CA that signed a server certificate, it will indicate that the connection is not secure. This is not necessarily a bad thing. It just indicates that the identity of the server you want to connect has not been verified. At this point, you can do one of two things: First, you can install the necessary root certificate on your client or browser. A lock icon in your browser's URL field will indicate the certificate was installed successfully. And second, you can install a self-signed certificate on your client. Unlike a root certificate, which is signed by a trusted CA, a self-signed certificate is signed by the person or entity that created it. While you can use a self-signed certificate to create an encrypted channel, understand that it carries an inherent amount of risk because the identity of the server you are connected with has not been verified.

Disable Insecure Ports and Services

As a general policy, any ports that are not needed should be disabled. You need to first know which ports are enabled, and then decide which of these ports can be safely disabled without disrupting the normal functioning of Cisco Crosswork. You can do this by listing the ports that are open and comparing it with a list of ports needed for Cisco Crosswork.

To view a list of all open listening ports:

Procedure

Step 1 Log in as a Linux CLI admin user and enter the **netstat -aln** command.
The **netstat -aln** command displays the server's currently open (enabled) TCP/UDP ports, the status of other services the system is using, and other security-related configuration information. The command returns output similar to the following:

```
[root@vm ~]# netstat -aln
Active Internet connections (servers and established)
Proto  Recv-Q   Send-Q   Local Address            Foreign Address         State
tcp    0        0        0.0.0.0:111              0.0.0.0:*               LISTEN
tcp    0        0        127.0.0.1:8080           0.0.0.0:*               LISTEN
tcp    0        0        0.0.0.0:22               0.0.0.0:*               LISTEN
tcp    0        0        127.0.0.1:25             0.0.0.0:*               LISTEN
tcp    0        0        127.0.0.1:10248          0.0.0.0:*               LISTEN
tcp    0        0        127.0.0.1:10249          0.0.0.0:*               LISTEN
```

```
tcp    0        0        192.168.125.114:40764    192.168.125.114:2379     ESTABLISHED
tcp    0        0        192.168.125.114:48714    192.168.125.114:10250    CLOSE_WAIT
tcp    0        0        192.168.125.114:40798    192.168.125.114:2379     ESTABLISHED
tcp    0        0        127.0.0.1:33392          127.0.0.1:8080           TIME_WAIT
tcp    0        0        192.168.125.114:40814    192.168.125.114:2379     ESTABLISHED
tcp    0        0        192.168.125.114:40780    192.168.125.114:2379     ESTABLISHED
tcp    0        0        127.0.0.1:8080           127.0.0.1:44276          ESTABLISHED
tcp    0        0        192.168.125.114:40836    192.168.125.114:2379     ESTABLISHED
tcp    0        0        192.168.125.114:40768    192.168.125.114:2379     ESTABLISHED
tcp    0        0        127.0.0.1:59434          127.0.0.1:8080           ESTABLISHED
tcp    0        0        192.168.125.114:40818    192.168.125.114:2379     ESTABLISHED
tcp    0        0        192.168.125.114:22       192.168.125.1:45837      ESTABLISHED
tcp    0        0        127.0.0.1:8080           127.0.0.1:48174          ESTABLISHED
tcp    0        0        127.0.0.1:49150          127.0.0.1:8080           ESTABLISHED
tcp    0        0        192.168.125.114:40816    192.168.125.114:2379     ESTABLISHED
tcp    0        0        192.168.125.114:55444    192.168.125.114:2379     ESTABLISHED
```

Step 2 Check the *Crosswork Network Controller 7.2 Installation Guide* for the table of ports used by Cisco Crosswork, and see if your ports are listed in that table. That table will help you understand which services are using the ports, and which services you do not need—and thus can be safely disabled. In this case, *safe* means you can *safely disable the port without any adverse effects to the product*.

Note
If you are not sure whether you should disable a port or service, contact the Cisco representative.

Step 3 If you have firewalls in your network, configure the firewalls to only allow traffic that is needed for Cisco Crosswork to operate.

Harden Your Storage

We recommend that you secure all storage elements that will participate in your Cisco Crosswork installation, such as the database, backup servers, and so on.

- If you are using external storage, contact the storage vendor and the Cisco representative.
- If you are using internal storage, contact the Cisco representative.
- If you ever uninstall or remove Cisco Crosswork, make sure that all VM-related files that might contain sensitive data are digitally shredded (as opposed to simply deleted). Contact the Cisco representative for more information.

Configure System Settings

Administrator users can configure the following system settings:

Configure a Syslog Server

Crosswork allows external syslog consumers to:

- Register on Crosswork to receive system events, audit events, and internal collection jobs from the Syslog and Trap servers.

- Define and filter which kind of events should be forwarded as a syslog, per consumer.
- Define the rate at which syslogs are forwarded to the consumer.

Note After the Syslog TLS server certificate is added, wait for 5-10 minutes before configuring the syslog server.

Attention The APIs to configure a syslog server are deprecated in the Crosswork 6.0 release.

Before you begin

Ensure that you have uploaded the Syslog TLS server certificate.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** tab.

Step 2 Under **Alarms and events settings**, click the **Notification destination** option.

Step 3 Click + to add the destination.

Step 4 In the **Add Destination** pane, from the **Destination** drop-down, select **Syslog receiver**.

Step 5 Enter the Syslog destination details. For more information, click ⓘ next to each option.

Step 6 If you have selected the **Protocol** as **TLS**, select the certificate from the **Syslog certificate** drop-down.

Step 7 Click **Save**.

Syslog Events

After the Syslog destination is configured, Crosswork generates events in the form of Syslogs and sends it to the Syslog destination. The events have the following format:

<pri><v> <stamp> <vip> <app> <PID> <Message ID> <Structure Data> <Message>

The following table lists the fields that are sent in syslogs.

Table 62: Syslog Event Fields and Description

Field	Description	Example

`Pri`	The priority of the event generated:
	`Priority = (8*facility + severity)`
	Where `facility` is the category of the event generated.
	The category of the event generated represented using an integer value:
	`System = 3, Network = 7, Audit = 13, Security = 4, External = 1`
	The alarm severity indicates the severity of the event using an integer value:
	`Critical=2, Major=3, Warning=4, Minor=5, Info=6,Clear=7`
		Event with the Category as System and Severity as Major, the Pri = 8 * 3 + 3 = 27.

`v`	The version of the Syslog server.	NA
`Stamp`	The timestamp at which the event is created.	`Mar 28 15:2:22 10.56.58.188`
`VIP`	The Crosswork VIP address.	`10.56.58.188`
`App`	The event OriginServiceId and OriginAppId.	`orchestrator-capp-infra`
`PID`	The process ID.	NA
`Message ID`	The event ID.	`8586f9cf-d05d-4d94-ab62-27d7e808b5f6`
`Structured Data`	The event ObjectId and event type.	`robot-topo-svc-0`
`Message`	The description of the event.	`Restart of robot-topo-svc successful.`

Configure a Trap Server

Cisco Crosswork allows external trap consumers to:

- Register on Crosswork and receive system events and audit log as traps.
- Define and filter which kind of events should be forwarded as traps, per consumer.
- Define the rate of which traps are forwarded to the consumer.

For more information on trap handling, see *<xref to Enable Trap Handling>*.

Attention The APIs to configure a trap server are deprecated in the Crosswork 6.0 release.

Follow the procedure below to manage Trap Servers from the Settings window:

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System settings** tab.

Step 2 Under **Alarms and events settings**, click the **Notification destination** option.

Step 3 Click + to add the destination.

Step 4 In the **Add Destination** pane, from the **Destination** drop-down, select **Trap receiver**.

Step 5 Enter Trap destination details. For more information, click ⓘ next to each option.

Step 6 After entering all the relevant information, click **Add**.

What to do next

Create a notification policy using the instructions in *<xref to Create Notification Policy for System Event>*.

Create Notification Policy for System Event

This topic explains the steps to create a notification policy for a system event.

For information on notification policies for Network or Device events, see *Set Up and Monitor Alarms and Events* section in the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management* guide.

Procedure

Step 1 From the main menu, choose **Alerts** > **Notification Policies**.

The **Notification Policies** window is displayed.

Step 2 Click **Create** and select **System/Network events**.

The **Create** window is displayed.

Step 3 Under **Policy Attributes**, enter relevant values for the following fields:

- Policy name
- Description
- Criteria

Note
If you do not want to specify any criteria, you can add an asterisk ('*') to the **Criteria** field.

Step 4 Click **Next**. Under **Destination**, select the destination(s) for the notification policy. The destination can be a trap receiver, syslog receiver, or an external kafka.

If there are no destinations available, click + to add a destination.

Step 5 Click **Next**. Review the summary details, and click **Save** to confirm the policy details.

Configure the Interface Data Collection

Crosswork Data Gateway collects the interface state and stats data such as name, type, and traffic counters from the devices through the SNMP or gNMI protocol. Crosswork Data Gateway starts the data collection when a device is onboarded and attached to the data gateway.

Follow the steps to configure interface data collection settings:

Before you begin

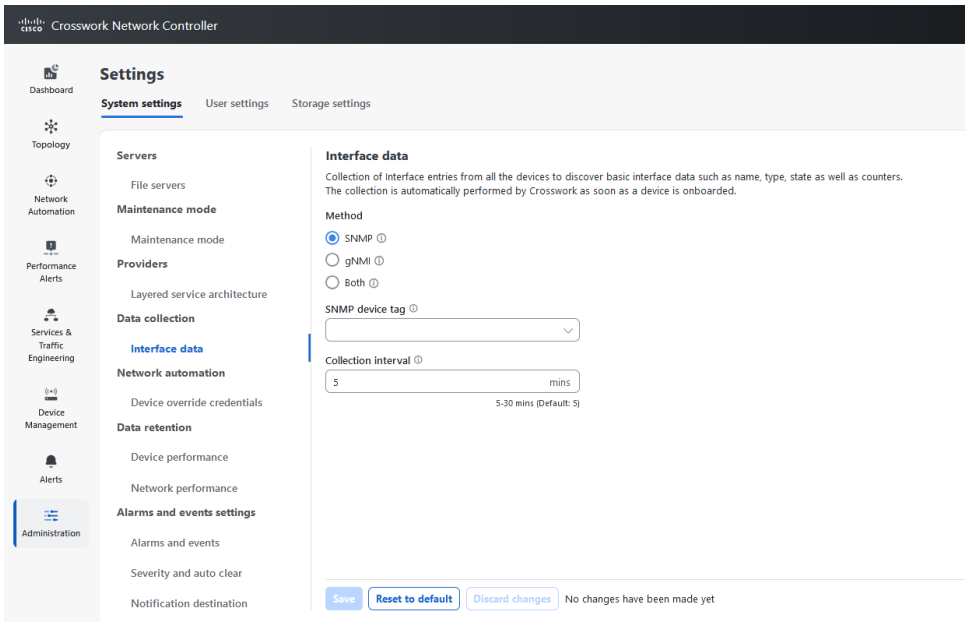
Create a tag and assign it to the device for which Crosswork collects the interface data. For information on how to create and assign a tag to the device, see Create tags and Apply or Remove Device Tags.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings** tab.

Step 2 Under **Data Collection**, select **Interfaces**.

Figure 89: Interface Data Window



Step 3 In the **Interface data** pane, select the appropriate method:

- SNMP: Crosswork collects the IF-MIB and IP-MIB data from the devices.
- gNMI: Crosswork collects the openconfig-interfaces data from the devices.
- Both: Depending on the device's capability, select SNMP and gNMI protocol to discover the devices.

If you choose **Both** as the method, you must select the appropriate SNMP and gNMI device tags. If you choose **SNMP** or **gNMI** method, the device tags become optional.

Step 4 From the **Select {SNMP or gNMI} Device Tag** drop-down, select unique tags for SNMP and gNMI protocols.

The precreated tags associated to the device are listed. If you select **No Tag Selected** option, Crosswork starts the data collection for devices with system SNMP or gNMI tags.

Step 5 In the **Interface Collection Interval** field, specify the duration between the data collection requests. The default duration is 5 minutes.

Step 6 Click **Save**.

Set the Pre-Login Disclaimer

Many organizations require that their systems display a disclaimer message in a banner before users login. The banner reminds the authorized users of their obligations when using the system, or provide warnings to unauthorized users. You can enable such a banner for Crosswork users, and customize the disclaimer message as needed.

Procedure

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings** tab.

Step 2 Under **Notifications**, click the **Pre-Login Disclaimer** option.

Step 3 To enable the disclaimer and customize the banner:

a) Check the **Enabled** check box.

b) Customize the banner **Title**, the **Icon**, and the **Disclaimer Text** as needed.

c) Optional: While editing the disclaimer, you can:

- Click **Preview** to see how your changes look when displayed before the Crosswork login prompt.
- Click **Discard Changes** to revert to the last saved version of the banner.
- Click **Reset** to revert to the original, default version of the banner.

d) When you are satisfied with your changes, click **Save** to save them and enable display of the custom disclaimer to all users.

Step 4 To turn off the disclaimer display: Select **Administration** > **Settings** > **System Settings** > **Pre-Login Disclaimer**, then uncheck the **Enabled** check box.

Manage File Server Settings

Cisco Crosswork provides secure file transfer services (FTP and SFTP) for Crosswork applications that need them. They are disabled by default.

Procedure

Step 1 To enable an FTP server:

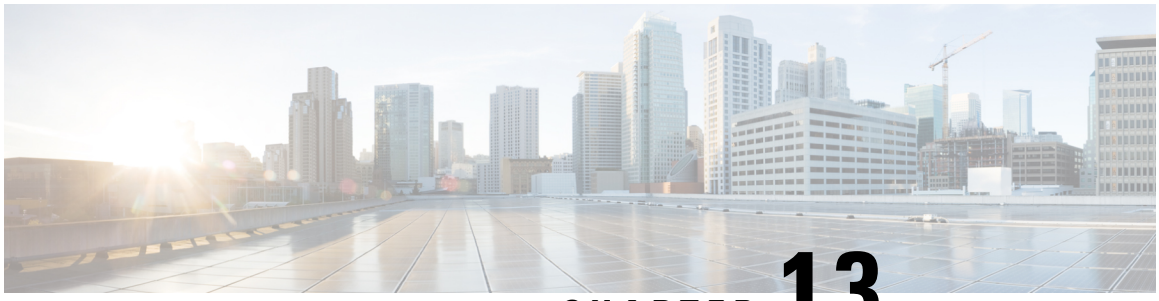
a) From the main menu, choose **Administration > Settings > System Settings > Servers > Filer Servers**.
b) Under FTP, select the **Enable FTP (Port TCP 30621)** check box.
c) Click **Save** to save your settings.

Step 2 To enable an SFTP server:

a) From the main menu, choose **Administration > Settings > System Settings > Servers > Filer Servers**.
b) Select the **Enable SFTP server upload Upload (Port TCP 30622)** check box.

Caution
SFTP supports an upload option that allows write access to the Cisco Crosswork storage from the outside. Use caution while enabling the upload, and it should be disabled as soon as it is no longer needed.

c) Click **Save** to save your settings.



CHAPTER 13

External Authentication Integration

External authentication integration in Crosswork enables secure user access management by connecting the platform to enterprise authentication systems such as TACACS+, LDAP, and RADIUS.

This chapter provides an overview of supported external authentication options, essential configuration principles, and the procedures required to control and monitor user sign-on through centralized authentication and authorization services.

User authentication systems

A user authentication system is a security feature that

- verifies user identities through external servers such as TACACS+, LDAP, or RADIUS,
- centralizes account and role management across the organization, and
- enables administrators to enforce consistent access policies for all users.

External authentication allows Crosswork Network Controller to delegate credential verification and role mapping to enterprise-grade services instead of relying solely on local accounts. By integrating with external authentication servers, you can align Crosswork Network Controller platform access with your organization's security standards. This integration also ensures scalable user management and supports regulatory compliance across teams.

Best practice for external server changes

Crosswork Network Controller supports configuration of up to 5 external authentication servers. When making changes to authentication server settings, observe the following recommendations:

- Perform all server additions, updates, or deletions in a single planned session to minimize user login disruptions.

- Ensure you have appropriate permissions before attempting to configure or delete external authentication servers.
- Wait a few minutes between consecutive changes to AAA server settings to avoid causing authentication errors or external login failures.
- Give write permission for remote authentication server APIs only to users who are authorized to manage or delete external authentication servers.
- After updating external server configuration in geo-redundant deployments, restart any standby appliance services as instructed by the documentation.
- Remember that changes to external authentication servers immediately affect all new user logins.

Configure TACACS+ servers

Add, update, or remove TACACS+ authentication servers to control user and device authentication in Crosswork Network Controller.

Crosswork Network Controller supports authentication of users via TACACS+ servers. You can integrate Crosswork with a standalone TACACS+ server (such as open TACACS+) or with an application like Cisco ISE (Identity Services Engine). Integrating with TACACS+ servers helps centralize and control access to network resources.

Before you begin

- Create a Device Access Group to manage access for AAA operations. For more information, see *<xref to Create Device Access Group>*
- In the TACACS+ server (standalone or Cisco ISE), configure required parameters such as user role, device access group attribute, shared secret format, and shared secret value before adding the server to Crosswork Network Controller.
- For details on configuring Cisco ISE, refer to the latest Cisco Identity Services Engine Administrator Guide.

Follow these steps to configure TACACS+ servers:

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **TACACS+** .

Step 2 To add a new TACACS+ server: Click  , enter required details (see TACACS+ field descriptions, on page 437), and click **Add**.

Step 3 To edit an existing TACACS+ server: Select the server you want to edit, click  , update required information, and click **Update**.

Step 4 To delete a TACACS+ server: Select the server you want to delete, click  , and confirm deletion.

Step 5 Click **Save** to apply the configuration. When prompted with a warning about restarting the server, click **Save changes** to confirm.

TACACS+ authentication servers are added, updated, or removed as configured. Crosswork uses these servers for user and device authentication.

What to do next

Test user authentication with the updated TACACS+ server settings to confirm successful configuration.

TACACS+ field descriptions

The table lists the key fields required when configuring a TACACS+ server in Crosswork Network Controller.

Table 63: TACACS+ field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the TACACS+ server (if IP address is selected).
DNS name	Enter the DNS name (if DNS name is selected). Only IPv4 DNS name is supported.
Port	The default TACACS+ port number is 49.
Shared secret format	Shared secret for the active TACACS+ server. Select ASCII or Hexadecimal.
Shared secret / Confirm shared secret	Plain-text shared secret for the active TACACS+ server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For Crosswork to communicate with the external authentication server, the **Shared Secret** parameter you enter on this screen must match with the shared secret value configured on the TACACS+ server.
Service	Enter the value of the service you are attempting to gain access to. This field is verified only for standalone TACACS+. In case of Cisco ISE, you can enter any value; do not leave the field blank. The service field is an attribute that tells the TACACS+ server what type of network service the user is trying to access. It allows the TACACS+ server to distinguish between different types of access, such as: • **Login access** (e.g., device CLI, SSH, console) • **Network access** (e.g., PPP, SLIP) For example, the "`raccess`" value is a service type used in the service field of an authorization request. It stands for **Remote Access** and is typically used when a user is requesting remote administrative access.

Field	Description
Policy ID	Enter the user role that you created in the TACACS+ server. The **Policy ID** is a unique key used by the TACACS+ server to identify and retrieve the user role assigned to an authenticated user. This value must exactly match the user role you configured on the TACACS+ server. In Crosswork Network Controller, this field corresponds to the *policy_id*. **Note** If you try to login to Crosswork Network Controller as a TACACS+ user before creating the required user role, you will get the error message: `"Key not authorized: no matching policy"`. If this occurs, close the browser. Login as a local admin user and create the missing user roles in the TACACS+ server, and login back to Crosswork using the TACACS+ user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the (ISE/Standalone) TACACS+ server attributes. These values can be one or more comma-separated entries. In a TACACS+ context, the Device Access Group attribute is typically a custom or authorization attribute that the TACACS+ server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy id to define user permissions across devices.
Retransmit timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.
Authentication type	Select the authentication type for TACACS+: • PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

Example

In this scenario, the TACACS+ parameters are configured in Cisco ISE.

- **Device Access Group** has already been created in Crosswork for AAA operation access.
- Relevant TACACS+ parameters configured in Cisco ISE:
  - **User profile**: `role0` (referenced in the **Policy Id** field)
  - **Device Access Group attribute**: `DAG-CONFIGURE`
  - **Shared secret format**: `ASCII`

Figure 90: Configure TACACS+ profile attributes in Cisco ISE

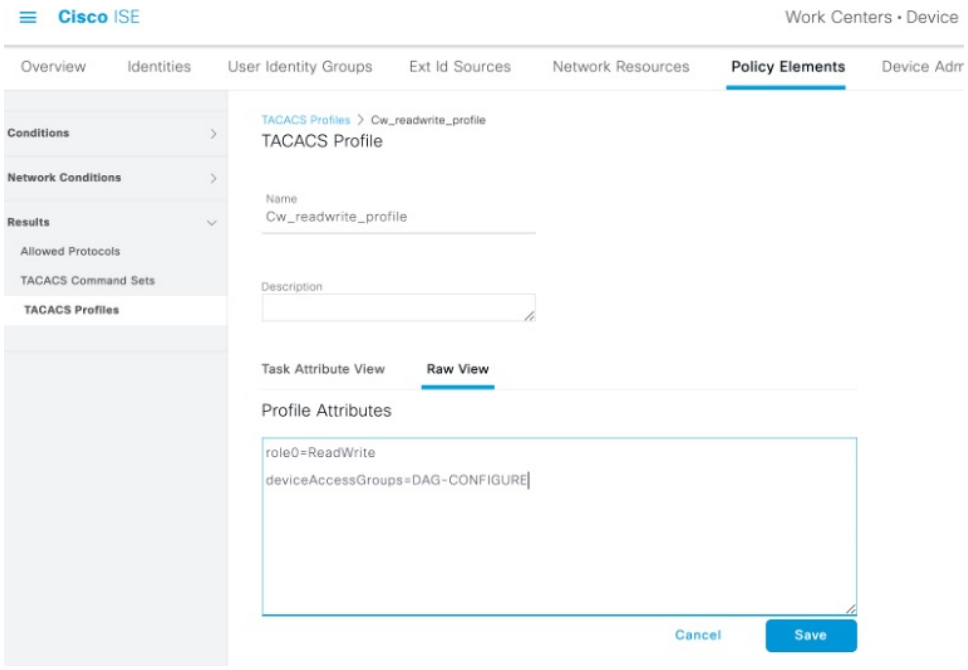
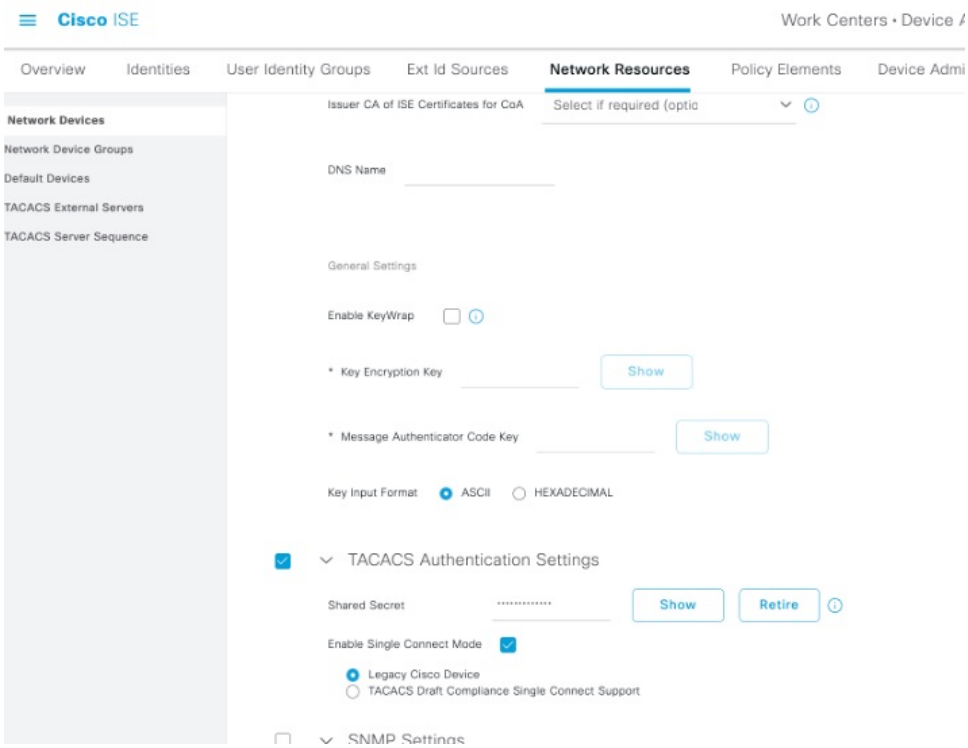
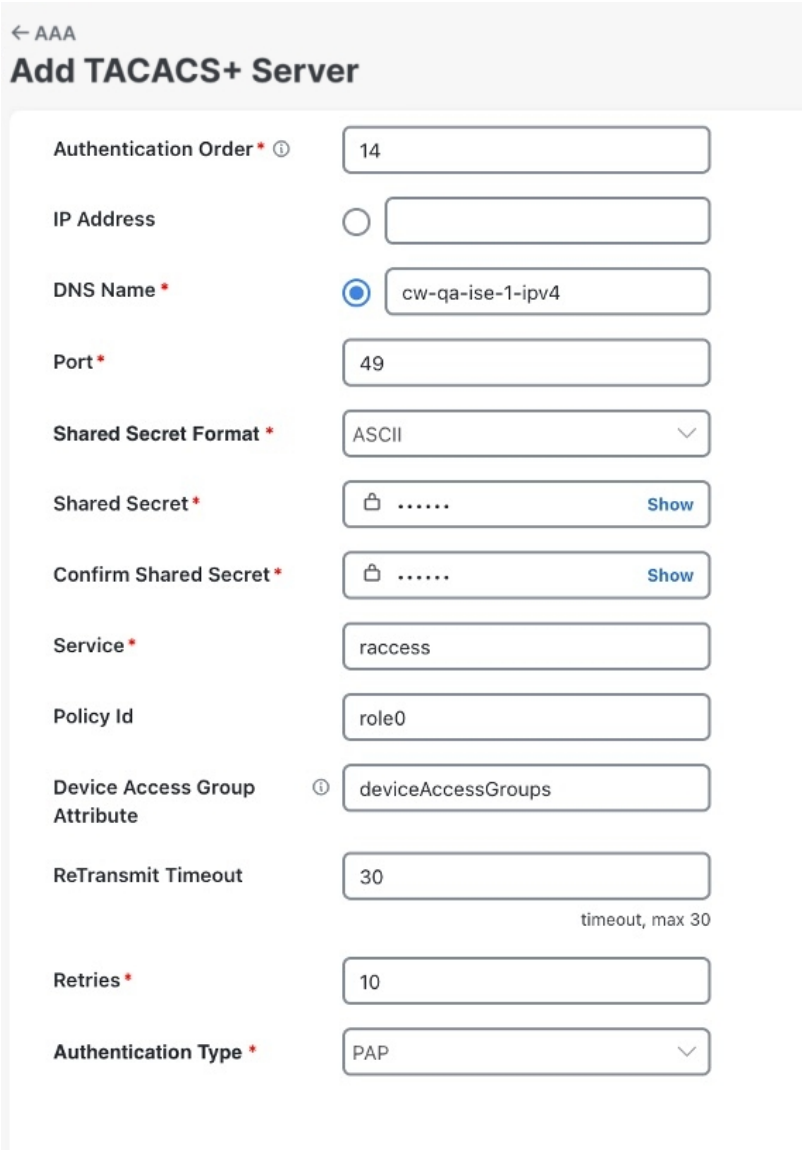


Figure 91: Configure TACACS+ authentication settings in Cisco ISE



Now, the TACACS+ server is added in Crosswork Network Controller UI:

Figure 92: Add TACACS+ server



API payload example

```
{
  "tacacs":{
    "tacacs_servers":[
    {
      "priority":10,
      "host":"cw-qa-ise-1-ipv4",
      "dnsName":"",
      "port":49,
      "secretFormat":"ascii",
      "secret":"sample",
      "service":"raccess",
      "policy-id": "role0",
```

```
      "virtualDomain":"deviceAccessGroups"
      "timeout":30,
      "retries":10,
      "authType":"pap",
    }
    ]
  }
}
```

Parameter mapping reference

```
Mapping reference:
-----------------------------------------------------------------------------------------------------------
Crosswork Network Controller                          CISCO ISE
VALUE
-----------------------------------------------------------------------------------------------------------
Device Access Group Attribute=deviceAccessGroups    deviceAccessGroups=DAG-CONFIGURE
DAG-CONFIGURE
PolicyId=role0                                      role0=ReadWrite
ReadWrite
```

Configure LDAP servers

Manage authentication connections by adding, editing, or deleting LDAP servers used for user authentication in Crosswork Network Controller.

Lightweight Directory Access Protocol (LDAP) servers, including OpenLDAP, Active Directory, and secure LDAP, are used to authenticate users for network management. Crosswork Network Controller can use these servers to centralize directory management and enforce access policies. Secure LDAP requires a certificate to enable encrypted communication.

Crosswork Network Controller supports two LDAP authentication modes:

- LDAP without Device Access Groups — LDAP returns a user-role attribute only.
- LDAP with Device Access Groups — LDAP returns both a user-role attribute and a device access group attribute. Crosswork Network Controller maps these values to configured roles and Device Access Groups.

LDAP attribute names shown in examples are for illustration only. Actual attribute names depend on your LDAP directory schema.

Before you begin

- Create a Device Access Group to manage access for AAA operations. For more information, see Create Device Access Groups, on page 415.
- Configure necessary parameters (such as bind DN, policy base DN, policy ID, and device access group attribute) on your LDAP server.
- For secure LDAP, add a "Secure LDAP Communication" certificate before proceeding. For details, see Add a new certificate, on page 377.
- Ensure your LDAP server is already configured to return the required attributes (role and, if applicable, device access group) before setting up LDAP in Crosswork Network Controller.

- LDAP attribute names vary across deployments; the attribute names shown in examples (such as **sAMAccountName**) come from an engineering test environment and may not exist in your LDAP setup.
- DN values shown in this guide (such as `OU=ouUsers1`, `dc=DSEENIVA`, etc.) reflect the example LDAP directory structure. Use DN values from your own LDAP environment.
- The device access group attribute returned by LDAP must match the configured Device Access Group name in Crosswork Network Controller.

Follow these steps to configure LDAP servers:

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **LDAP** .

Step 2 To add a new LDAP server: Click  , enter required details (see TACACS+ field descriptions, on page 437), and click **Add**.

Step 3 To edit an existing LDAP server: Select the server you want to edit, click  , update required information, and click **Update**.

Step 4 To delete a LDAP server: Select the server you want to delete, click  , and confirm deletion.

Step 5 Click **Save** to apply the configuration. When prompted with a warning about restarting the server, click **Save changes** to confirm.

LDAP authentication servers are added, updated, or removed, and the changes are applied to authentication services in Crosswork Network Controller.

What to do next

Confirm the server is correctly listed and test user authentication if applicable.

LDAP field descriptions

The table lists the key fields that are required when you configure an LDAP server in Crosswork Network Controller.

Table 64: LDAP field descriptions

Field	Description
Authentication order	Defines the priority used when processing authentication requests. Accepts values from **10 to 99**; values below 10 are reserved for system use. The default value is **10**.
Name	A label used to identify the LDAP handler.
IP address/host name	The IP address or fully qualified hostname of the LDAP server.

Field	Description
Secure connection	Enables SSL-based LDAP communication. When selected, you must choose a **Secure LDAP Communication** certificate from the drop-down list. This field is disabled by default. **Note** The certificate must already exist in the Certificate Management screen before enabling secure LDAP.
Port	Specifies the port used to connect to the LDAP server. The default LDAP port is **389**. When secure LDAP is enabled, the default port is **636**.
Bind DN	The distinguished name (DN) used by Crosswork Network Controller to bind to the LDAP server for authentication queries.
Bind credential / Confirm bind credential	The username and password used to authenticate the Bind DN with the LDAP server.
Base DN	The starting point in the LDAP directory tree where Crosswork performs its user search operations.
User filter	The LDAP search filter used to locate user entries within the Base DN.
DN format	Specifies how user names are represented within the Base DN. This determines how Crosswork constructs the full DN for authentication queries.
Principal attribute ID	The attribute in the LDAP user profile that stores the user identifier (UID).
Policy base DN	The directory location used for role lookup and role mapping.
Policy map attribute	Identifies the attribute in the Policy base DN used to map a user to a specific role. This corresponds to the **userFilter** attribute on the LDAP server.
Policy ID	Specifies the role value returned by LDAP for the authenticated user. This value must match a corresponding user role configured on the LDAP server. In Crosswork Network Controller, this field maps to **policy_id**. **Note** If a user logs into Crosswork Network Controller before the required role exists on the LDAP server, authentication fails with: *"Login failed, policy not found. Please contact the Network Administrator for assistance."* Ensure LDAP roles are created before adding the LDAP server configuration in Crosswork Network Controller.
Device access group attribute	Specifies the LDAP attribute used to identify the user's device access group. This may include one or more comma-separated values. In LDAP environments, this attribute is typically a custom authorization value returned to the client. The returned value must correspond to an existing Device Access Group in Crosswork.
Connection timeout	Time (in seconds) allowed for LDAP operations to complete. The maximum allowed value is **30 seconds**.

LDAP example

This example shows parameters used for secure LDAP configuration. A Device Access Group named `"ALL-ACCESS"` is already configured in Crosswork Network Controller and referenced in LDAP.

Key points from the LDAP server configuration:

- The user role is **ldapa-user1**, part of the **ldapAdmin** group.
- The username is **DSEENIVA**.
- The policy ID returned by LDAP is **sAMAccountName**.
- `ldapUrl` contains the server hostname and port.
- In `ldap_attr_server` fields:
  - `baseDN` corresponds to **Policy base DN**.
  - `userFilter` corresponds to **Policy map attribute**.
- Device access group is returned via: `Description='ALL-ACCESS'`.

API payload example

DN samples used in the example (such as `dc=DSEENIVA,dc=COM` or `OU=ouUsers1`) reflect only the example directory's structure. Use the DN values from your LDAP environment.

Attention The following example is the LDAP server's response used during testing. It is not the CNC API request payload. Attribute names and DN structure are specific to that test environment. Use your own directory's attribute names and values when configuring LDAP.

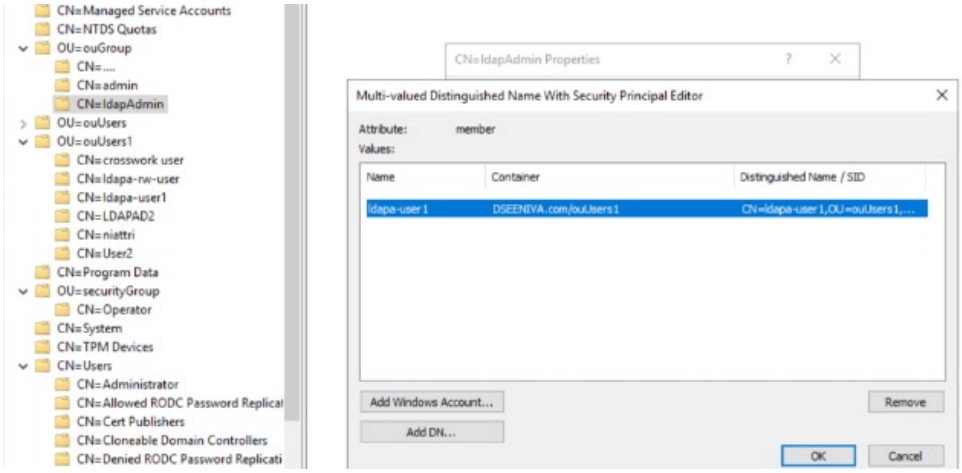
```
json:Y

{   "ldap": {
    "ldap_servers": {
      "ldap_server": [{
          "type": "DIRECT",
          "bindDn": "cn=ldapa-user1,OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "connectionStrategy": "",
          "useSsl": false,
          "useStartTls": false,
          "connectTimeout": 10,
          "baseDn": "OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "userFilter": "cn={user}",
          "subtreeSearch": true,
          "usePasswordPolicy": false,
          "dnFormat": "cn=%s,OU=ouUsers1,dc=DSEENIVA,dc=COM",
          "principalAttributeId": "cn",
          "policyId": "Description",
          "minPoolSize": 1,
          "maxPoolSize": 1,
          "validateOnCheckout": false,
          "validatePeriodically": true,
          "validatePeriod": 600,
          "idleTime": 5000,
          "prunePeriod": 5000,
          "blockWaitTime": 5000,
```

```
    "providerClass": "org.ldaptive.provider.unboundid.UnboundIDProvider",
    "allowMultipleDns": false,
    "order": 16,
    "trustStore": "ldaps",
    "name": "ldapsecure",
    "ldapUrl": "ldaps://cw-qa-ldap-2-ipv4:636",
    "bindCredential": "<>"
  }
],
"ldap_attr_servers": {
  "ldap_attr_server": [
    {
      "baseDn": "OU=ouGroup,dc=DSEENIVA,dc=COM",
      "trustStore": "ldaps",
      "ldapUrl": "ldaps://cw-qa-ldap-2-ipv4:636",
      "bindDn": "cn=ldapa-user1,OU=ouUsers1,dc=DSEENIVA,dc=COM",
      "bindCredential": "<>",
      "userFilter": "member=cn={user},OU=ouUsers1,dc=DSEENIVA,dc=COM",
      "failFast": false,
      "attributes": {
      "policy_id":"sAMAccountName"
      }}]}}}
```

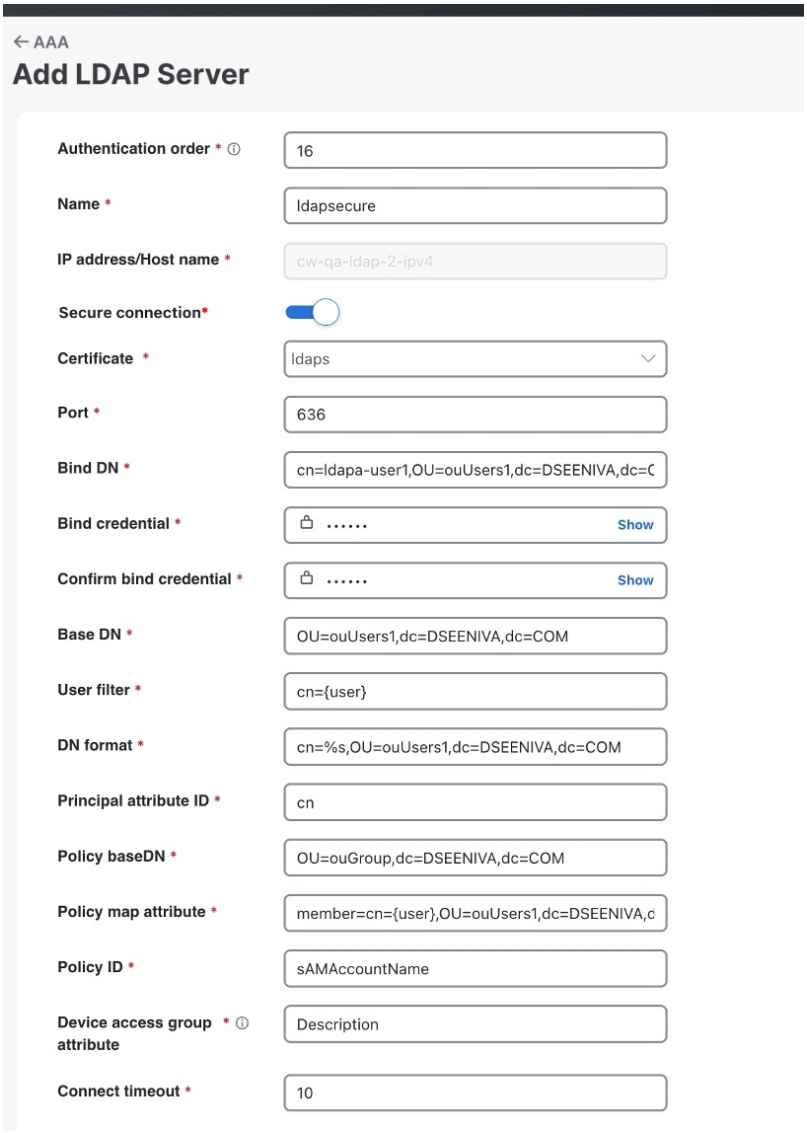

The user group and user role mapping configured in LDAP server:

Figure 93: Map user group and user role in LDAP server



Here is the corresponding LDAP configuration in the Crosswork Network Controller UI:

Figure 94: Add LDAP server



Configure RADIUS servers

Add, edit, or delete RADIUS servers to enable centralized user authentication and authorization in Cisco Crosswork.

Crosswork uses RADIUS (Remote Authentication Dial-In User Service) servers to authenticate users. You can integrate Crosswork with applications such as Cisco Identity Services Engine (ISE) for RADIUS-based authentication.

Before you begin

- Create a Device Access Group to manage access for AAA operations. For more information, see *<xref to Create Device Access Group>*

- In the RADIUS server (standalone or Cisco ISE), configure required parameters such as user role, device access group attribute, shared secret format, and shared secret value before adding the server to Crosswork Network Controller.
- For details on configuring Cisco ISE, refer to the latest Cisco Identity Services Engine Administrator Guide.

Follow these steps to configure RADIUS servers:

Procedure

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **RADIUS** .

Step 2 To add a new RADIUS server: Click  , enter required details (see RADIUS field descriptions, on page 447), and click **Add**.

Step 3 To edit an existing RADIUS server: Select the server you want to edit, click  , update required information, and click **Update**.

Step 4 To delete a RADIUS server: Select the server you want to delete, click  , and confirm deletion.

Step 5 Click **Save** to apply the configuration. When prompted with a warning about restarting the server, click **Save changes** to confirm.

RADIUS authentication servers are added, updated, or removed as configured. Crosswork uses these servers for user and device authentication.

What to do next

Test user authentication with the updated RADIUS server settings to confirm successful configuration.

RADIUS field descriptions

The following table describes the key fields required when configuring a RADIUS server in Crosswork Network Controller:

Table 65: RADIUS field descriptions

Field	Description
Authentication order	Specify a unique priority value to assign precedence in the authentication request. The order can be any number between 10 to 99. Below 10 are system reserved. By default, 10 is selected.
IP address	Enter the IP address of the RADIUS server (if IP address is selected).
DNS name	Only IPv4 DNS name is supported (if DNS name is selected).
Port	The default RADIUS port number is 1645.
Shared secret format	Shared secret for the active RADIUS server. Select ASCII or Hexadecimal.

Field	Description
Shared secret / Confirm shared secret	Plain-text shared secret for the active RADIUS server. The format of the text entered must match with the format selected (ASCII or Hexadecimal). For Crosswork to communicate with the external authentication server, the **Shared Secret** parameter you enter on this screen must match with the shared secret value configured on the RADIUS server.
Service	Enter the value of the service you are attempting to gain access to. The service field is an attribute that tells the RADIUS server what type of network service the user is trying to access. It allows the RADIUS server to distinguish between different types of access, such as: • **Login access** (e.g., device CLI, SSH, console) • **Network access** (e.g., PPP, SLIP) For example, the "`raccess`" value is a service type used in the service field of an authorization request. It stands for **Remote Access** and is typically used when a user is requesting remote administrative access.
Policy ID	Enter the user role that you created in the RADIUS server. The **Policy ID** is a unique key used by the RADIUS server to identify and retrieve the user role assigned to an authenticated user. This value must exactly match the user role you configured on the RADIUS server. In Crosswork Network Controller, this field corresponds to the *policy_id*. **Note** If you try to login to Crosswork Network Controller as a RADIUS user before creating the required user role, you will get the error message: "`Key not authorized: no matching policy`". If this occurs, close the browser. Login as a local admin user and create the missing user roles in the RADIUS server, and login back to Crosswork using the RADIUS user credentials.
Device access group attribute	Enter the device access group attribute value based on the key used for the device access group in the RADIUS server attributes. These values can be one or more comma-separated entries. In a RADIUS context, the Device Access Group attribute is typically a custom or authorization attribute that the RADIUS server sends back to the network device. This attribute specifies which group of network devices or which level of device access policy applies to the authenticated user. The Device Access Group attribute works in sync with the policy id to define user permissions across devices.
Retransmit timeout	Enter the timeout value. Maximum timeout is 30 seconds.
Retries	Specify the number of authentication retries allowed.

Field	Description
Authentication type	Select the authentication type for RADIUS: • PAP: Password-based authentication is the protocol where two entities share a password in advance and use the password as the basis of authentication. • CHAP: Challenge-Handshake Authentication Protocol requires that both the client and server know the plain text of the secret, although it is never sent over the network. CHAP provides greater security than Password Authentication Protocol (PAP).

Configure AAA settings

Control user authentication, authorization, and accounting on the system by configuring AAA settings to enforce security policies and manage user sessions.

Users with relevant AAA permissions can configure the AAA settings.

Configure these settings when you need to establish or update how users are authenticated, what resources they can access, and how their activities are tracked. Proper AAA settings help safeguard network resources and ensure compliance with organizational access policies.

Before you begin

- Ensure you have administrator permissions or equivalent AAA configuration rights.
- Review your organization's authentication and password policy requirements.
- Gather information about external authentication servers (if applicable).
- Notify affected users of possible session interruptions during configuration changes.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **Settings** .

Step 2 Select the relevant setting for **Fallback to local**. By default, Crosswork Network Controller prefers external authentication servers over local database authentication.

Note
Admin users are always authenticated locally.

Step 3 Under **Browser session timeout**, select the relevant value for the **Log out inactive users after** field. Any user who remains idle beyond the specified limit will be automatically logged out.

This timeout is enforced by the system and applies even if the user closes the browser tab without explicitly logging out. If no activity (token usage) is detected after the tab is closed, the session expires after the configured timeout. For example, with a 10-minute timeout, if a user closes the browser tab after 5 minutes of activity, the user must log in again if they return after 10 minutes.

Note

- The default timeout value is 30 minutes.
- Changes to the timeout value take effect immediately, including for active sessions.
- Session termination can take upto a minute more than the configured timeout due to backend scheduling.
- This setting applies only to browser-based UI sessions. API-based sessions continue to follow the existing 8-hour validity behavior.

Step 4 Under **Parallel session**, enter relevant values for the **Number of parallel sessions** and **Number of parallel sessions per user** fields.

Note
Crosswork Network Controller supports between 5 to 200 parallel session for concurrent users. If the number of parallel sessions are exceeded, an error is displayed while logging in to Crosswork Network Controller .

Note
Crosswork Network Controller supports 50 simultaneous NBI sessions up to 400 sessions.

Step 5 Under **Source IP**, enable auditing of user source IP addresses.

a) Select the **Enable source IP for auditing** checkbox to log the user's source IP address for auditing and accounting. This option is disabled by default.
b) Log out, wait a few minutes, then log back in. This pause ensures the change is applied and the actual client IP address is accurately captured.

   During this transition, audit logs may temporarily display the Crosswork node IP instead of the client IP. The correct client IP will appear in new audit log entries created after you log in again. Previous log entries will continue to show the node IP. Once enabled and you have logged in again, the **Source IP** column will appear on both the **Audit Log** and **Active sessions** pages.

Step 6 Select the relevant settings for the **Local password policy**. Certain password settings are enabled by default and cannot be disabled (for example, Change password on first login).

Note
Any changes in the password policy is enforced only the next time when the users change their password. Existing passwords are not checked for compliance during login.

Note
Local password policy allows administrators to configure the number of unsuccessful login attempts a user can make before they are locked out of Crosswork Network Controller , and the lockout duration. Users can attempt to login with the correct credentials once the wait time is over.

Enable single sign-on

Enable single sign-on (SSO) so users can access multiple related applications with a single set of credentials, streamlining authentication and simplifying navigation between service providers.

Single sign-on (SSO) is an authentication method that lets users log in once and access multiple independent systems without reentering credentials. Crosswork Network Controller acts as an Identity Provider (IdP) and

supports SSO integration for service provider applications. You can enable SSO for users authenticated via TACACS+, LDAP, and RADIUS. When SSO is configured, users benefit from seamless access and improved security management.

Crosswork Network Controller also supports SSO cross-launch, so users can move easily between Crosswork Network Controller and integrated applications. Once configured, the URL can be launched using the launch icon ( ) located at the top right corner of the window.

Note that the Crosswork Network Controller login page is not shown if the Central Authentication Service (CAS) pod is restarting or offline.

Attention

- When Crosswork Network Controller's CAS pod is restarting or not running, the login page is not available.
- The SSO URL from the Identity Provider (IdP) is *https://<IP>:30603/crosswork/sso/idp/profile/SAML2/Redirect/SSO*, where <IP> represents the Crosswork Network Controller's IP address or hostname.

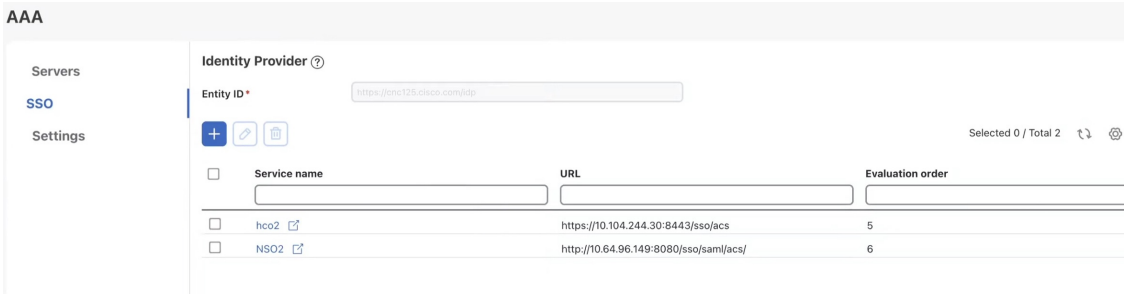
Before you begin

- Select **Enable source IP for auditing** check box on the **Administration** > **AAA** > **Settings** page.
- Ensure you have the latest service provider metadata to integrate with Crosswork Network Controller SSO.
- Confirm that network connectivity exists between Crosswork Network Controller (IdP) and each service provider application.
- Verify the CAS pod is running and stable.

Procedure

Step 1 From the main menu, choose **Administration** > **AAA** > **SSO** . The **Identity Provider** window appears. You can add, edit or delete SSO providers here.

Figure 95: Identity Provider window



Step 2 To add a new service provider:

a) Click the icon.

b) In the **Service Provider** window, enter the values in the following fields:

- **Name**: Specify the entity name.
- **Evaluation order**: Assign a unique number for service definition priority.
- **Metadata**: Provide or browse to the SAML metadata XML document for the service provider.

Note
If you supply a URL, the **Service name** entry becomes a hyperlink for cross-launch.

c) Click **Add** to confirm.

Step 3 Click **Save all changes**. When prompted, confirm by clicking **Save changes**.

Note
Saving changes may require restarting the server for updates to take effect.

After the settings are saved, when you log into the integrated service provider application for the first time, the application gets redirected to the Crosswork Network Controller server. After providing the Crosswork credentials, the service provider application logs in automatically. For all the subsequent application logins, you do not have to enter any authentication details.

Step 4 To edit a service provider:

a) Select the check box next to the service provider, then click the icon.
b) Update evaluation order or metadata information as needed.
c) Click **Update** to apply changes.

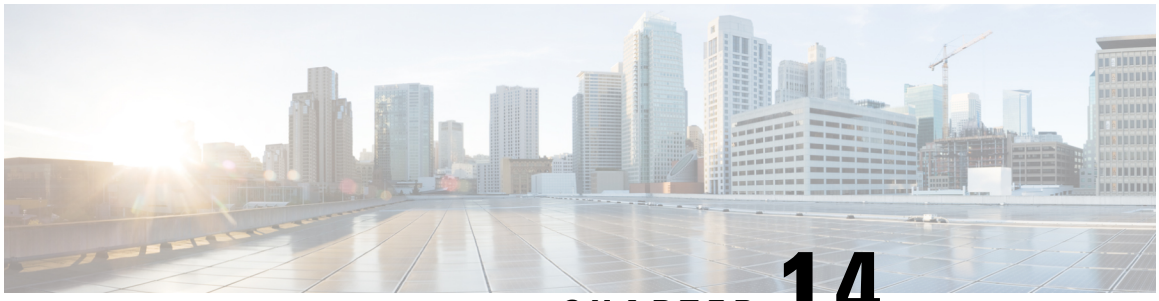
Step 5 To delete a service provider:

a) Select the check box next to the service provider, then click the icon.
b) Click **Delete** to confirm removal.

Single sign-on is enabled for selected service provider applications. Users can authenticate once via Crosswork Network Controller and seamlessly access associated applications without reentering authentication factors.

What to do next

- If Crosswork Network Controller is reinstalled or migrated, update the Identity Provider (IdP) metadata in all service provider applications to avoid authentication errors due to metadata mismatch.
- For first-time users, ensure password change is completed before attempting to log in with a different username. To reset an incomplete session, an administrator must terminate it.



CHAPTER 14

Manage System Health

This section contains the following topics:

Monitor system and application health

The health of the Crosswork Platform system and applications is determined by the operational status of its microservices.

- The system is considered healthy if all services are up and running.
- The health is considered degraded if one or more services are down.
- The health status is down if all services are down.

Monitoring System and Application Health in Crosswork Platform

The Crosswork Platform is built on an architecture consisting of microservices. These microservices, create dependencies across various services within the Crosswork system.

To monitor system and application health, from the main menu, choose **Crosswork Manager** to access the **Crosswork Summary** and **Crosswork Health** windows. Each window provides different views to help you monitor system and application health. You can use the tools and information provided in this window, along with support and guidance from your Cisco Customer Experience account team. Also, you can use the tools to identify, diagnose, and fix issues with the Cisco Crosswork cluster, Platform Infrastructure, and installed applications.

While both windows can give you access to the same type of information, the purpose of each summary and view is different.

Monitor cluster health

The Monitor Cluster Health feature provides a summary of the overall system health, focusing on hardware resources and virtual machines (VMs).

- Displays system health at a glance in the **Crosswork Summary** window.
- Allows users to check hardware resource status and VM performance before installing or upgrading applications.
- Enables users to view resource utilization, drill down on VMs, and perform VM or cluster-related activities.

Accessing and Using Cluster Health Information

The **Crosswork Summary** window, accessible via **Crosswork Manager** > **Crosswork Summary**, provides a summary of system health. Users can click the **System Summary** tile to view resource utilization and manage VMs or cluster-related activities. If hardware resources are overutilized or services are degrading, users may need to add more VMs to scale the system. Additional details, such as microservices and alarms, can be accessed by clicking on the **Cisco Crosswork Platform Infrastructure** and application tiles.

For more information, see Cluster management overview.

Monitor platform infrastructure and application health

The **Crosswork health** window (**Crosswork Manager** > **Crosswork health** tab) displays summaries for the Crosswork platform infrastructure health and installed applications status, with details of microservice status.

Within the **Crosswork health** tab, you can perform these actions:

- Click the ··· icon on the application row to view application details.
- Expand an application row to view information on microservices, alarms, and events for the selected Crosswork product.

From the **Microservices** tab, you can:

- View the list of microservices and, if applicable, associated microservices by clicking on the microservice name.
- Click ··· to restart or obtain Showtech data and logs for each microservice.

Note Showtech logs must be collected separately for each application.

From the **Alarms** tab, you can:

- Filter the active alarms.
- Click the alarm description to drill down on alarm details.
- Change the status of the alarms (Acknowledge, Unacknowledge, Clear).
- Add notes to alarms.
- View list of events in the product.
- View the correlated alarm for each event.

Visually monitor system functions in real time

You can monitor the health of Crosswork Network Controller and any of its functions in real time, using a set of monitoring dashboards you can access from the **Crosswork Manager** window.

Crosswork Network Controller uses Grafana to create these dashboards. The dashboards display the graphical view of the product's infrastructure, using metrics collected in its database. You can use these dashboards to diagnose problems you may encounter with individual Crosswork Network Controller applications or their underlying services.

There are multiple monitor dashboards. Each dashboard is categorized by the type of functionality it monitors and the metrics it provides. This table lists some categories that may be available depending on which Crosswork Network Controller applications are installed.

Table 66: Monitoring dashboard categories

This dashboard category...	Monitors...
Change Automation	Playbook functions. Metrics include the number of MOP jobs executed, response latency, API calls, database activity, and so on.
Optima	Feature pack, traffic, and SR-PCE dispatcher functions.
Collection - Manager	Device-data collection functions. Metrics include telemetry collection latencies, total collection operations, memory and database activity related to telemetry, delayed collections, and so on.
Health Insights	Key Performance Indicator functions. Metrics include the number of KPI alerts, API calls, and so on.
Infra	System infrastructure messaging and database activity.
Inventory	Inventory manager functions. These metrics include total numbers of inventory change activities.
Platform	System hardware and communications usage and performance. Metrics include disk and CPU usage, database size, network and disk operations, and client/server communications.
ZTP	Zero Touch Provisioning functions.

To conserve disk space, Crosswork Network Controller maintains a maximum of 24 hours of collected metric data.

Grafana is an open-source visualization tool. This section provides general information about how to use the Crosswork Network Controller implementation of Grafana. For more information about Grafana itself, see https://grafana.com and http://docs.grafana.org

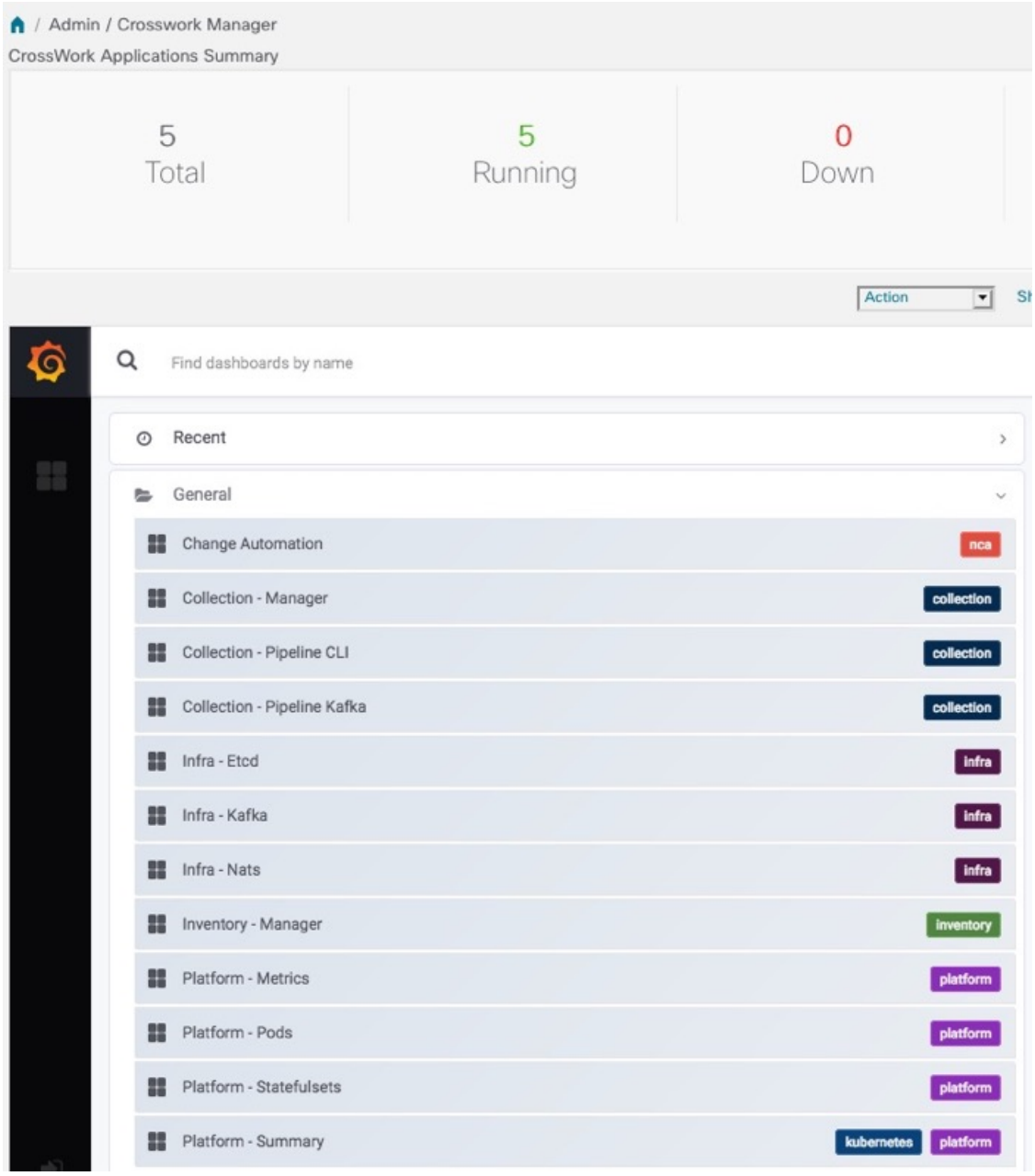
Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager** > **System Summary**.

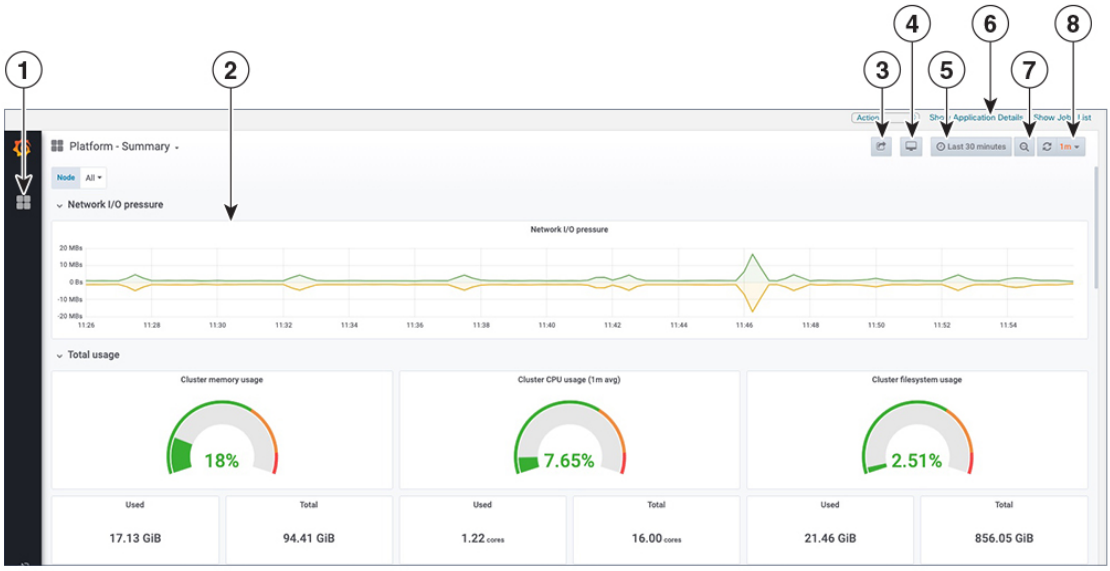
Step 2 At the top right, click **View More Visualizations**.

The Grafana user interface appears.

Step 3 In the Grafana user interface, click **Home**. Grafana displays the list of monitoring dashboards and their categories, as shown in this example.



Step 4 Click the dashboard you want to view. For example, when you click on **Platform - Summary** dashboard, a view appears similar to one shown in the next figure.



Step 5 Scroll the dashboard to display all the metrics, or select any of the functions described in the following table.

Item	Description
1	**Dashboard Icon**: Click the icon to re-display the dashboard list and select a different dashboard.
2	**Time Series Graph Zoom**: You can zoom in on a specific time period within the graph of any time series data, as follows: **a.** Click a time-period starting point in the graph line and hold down the mouse. **b.** Drag the cursor to the endpoint. Light gray shading appears in the block you are selecting. When you reach the endpoint, release the mouse. To reset a zoomed time series graph to the default, click the **Zoom Out icon**.
3	**Share Dashboard icon**: Click the icon to make the dashboard you are viewing shareable with other users. Clicking this icon displays a pop-up window with tabs and options to share the dashboard in your choice of these forms: • **URL Link**: Click the **Link** tab and then click **Copy** to copy the dashboard's URL to your clipboard. You can also choose whether to retain the current time and template settings with the URL. • **Local Snapshot File**: Click the **Snapshot** tab and then click **Local Snapshot**. Grafana creates a local snapshot of the dashboard on the server. When the snapshot is ready, click **Copy Link** to copy the URL of the snapshot to your clipboard. • **Export to JSON File**: Click the **Export** tab and then click **Save to file**. You will be prompted to save or open the exported JSON file. You can also choose to turn data source names in the file into templates by selecting the **Export for sharing externally** checkbox before clicking **Save to file**. • **View JSON File and Copy to Clipboard**: Click the **Export** tab and then click **View JSON** (you can choose to templatize data source names by selecting the **Export for sharing externally** checkbox before clicking **View JSON**). Grafana displays the exported JSON code in a popup window. Click **Copy to Clipboard** to copy the file to your clipboard.

Item	Description
4	**Cycle View Mode icon**: Click this icon to toggle between the default Grafana **TV** view mode and the **Kiosk** mode. The **Kiosk** view hides most of the Grafana menu. Press **Esc** to exit the **Kiosk** view.
5	**Time/Refresh Selector**: Indicates the time period for the metrics displayed in the dashboard and how often the metrics are refreshed. Click the selector to choose a different time range and refresh rate. You can specify a custom pair of time-range start and end points, or choose from one of several predefined ranges, such as **Last 30 minutes** or **Last 3 hours**. When you have finished making changes, click **Apply**. **Note** When making selections, remember only the last 24 hours of data is stored. If you select time ranges beyond that limit, the dashboard may be blank.
6	**Show Application Details**: Click this option to view details of the selected dashboard item.
7	**Zoom Out icon**: Click this icon to reset a zoomed time series graph back to the unzoomed state.
8	**Refresh icon**: Click this icon to immediately or choose time interval to refresh the data shown. You can choose predefined refresh rates from **Off** to **2 Days**.

Check system health

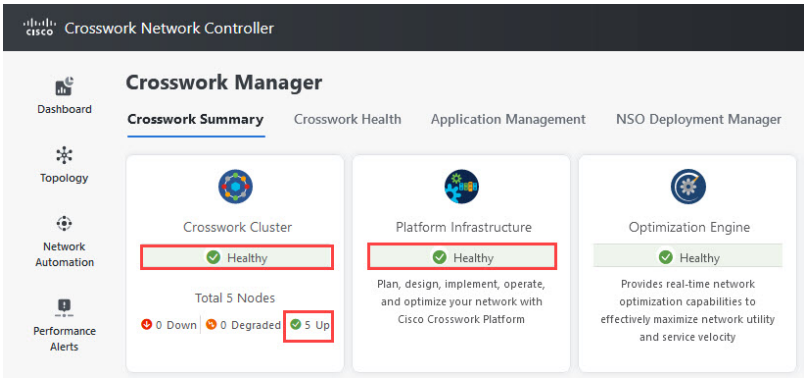
In this example, you can navigate through the different windows and identify areas to check for a healthy Crosswork system.

Procedure

Step 1 Check overall system health.

- From the main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary** tab.
- Check that all the nodes are in operational state (Up) and that the Crosswork Cluster and Platform Infrastructure is healthy.

Figure 96: Crosswork Summary



Step 2 Check and view detailed information about the microservices that run as part of the Crosswork Platform Infrastructure.

- Click the **Crosswork Health** tab.
- Expand the Crosswork Platform Infrastructure row, click ⋯, and select **Application Details**.
- From the **Application Details** window, you can check and review microservice details, restart microservices, and collect showtech information. You can also perform installation-related tasks from this window.

Figure 97: Crosswork Health

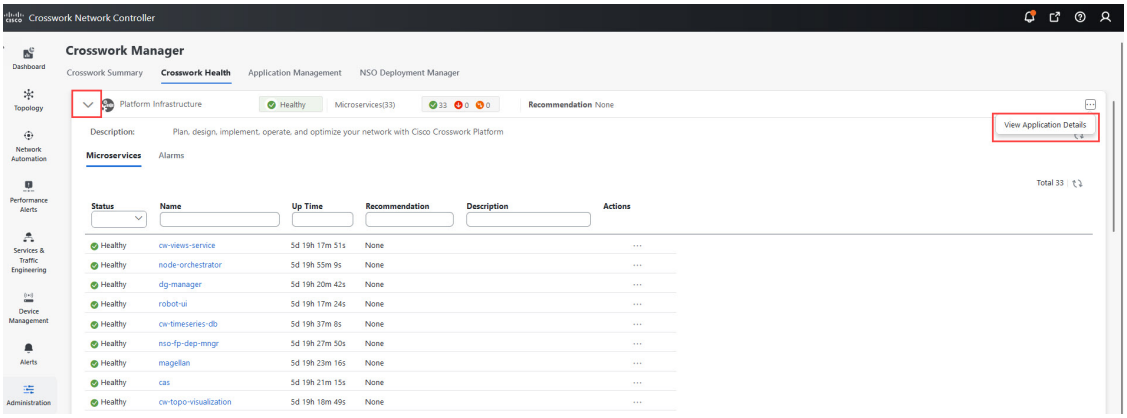
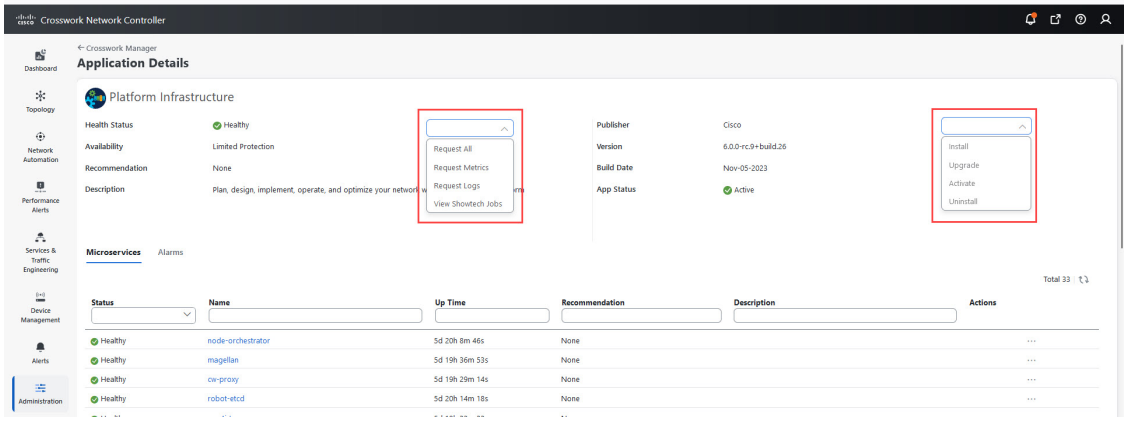


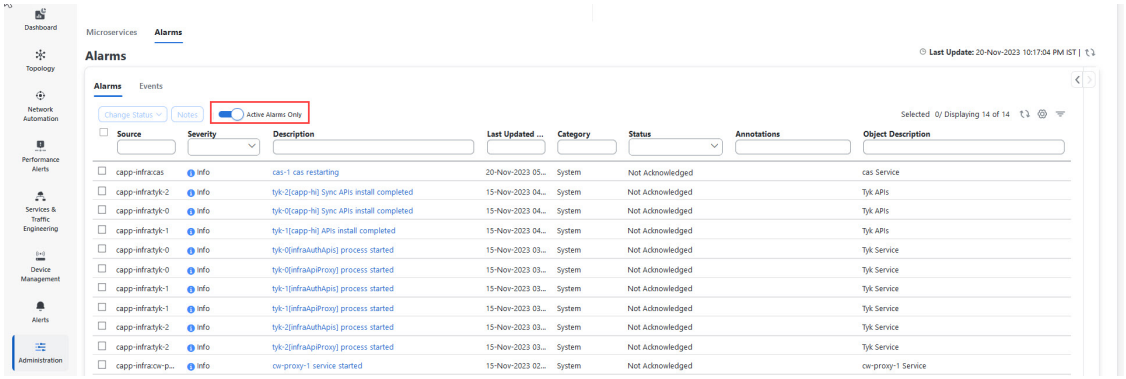
Figure 98: Application Details



Step 3 Check and view the alarms and events related to the microservices.

- Click the **Alarms** tab. The list displays only Crosswork Platform Infrastructure alarms. You can further filter the list by viewing only active alarms.
- Click the **Events** tab. The list displays all Crosswork Platform Infrastructure events, and their corresponding alarms.

Figure 99: Alarms



Step 4 View which Crosswork applications are installed.

- From the main menu, choose **Administration** > **Crosswork Manager** > **Application Management** tab and click **Applications**. This window displays all applications that have been installed. You can also click **Add new file** to install more applications by uploading another application bundle or an auto-install file.

Step 5 View the status of jobs.

- Click the **Job History** tab. This window provides the information regarding the status of jobs and the sequence of events that have been executed as part of the job process.

Alarms and events window

The **Alarms and Events** window in Crosswork Network Controller provides a centralized interface to view, filter, and manage system alarms and events.

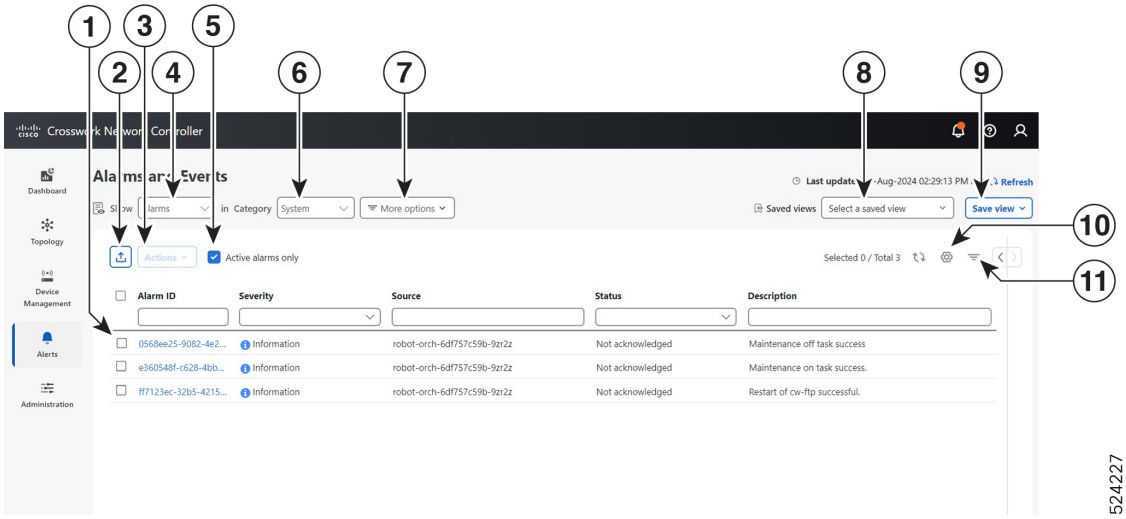
You can view the **Alarms and Events** by navigating to one of the following:

- From the main Crosswork window, click .
- From the main menu, choose **Alerts** > **Alarms and Events**.

Note For information on Network or Device alarms, see *Set Up and Monitor Alarms and Events* section in the *Cisco Crosswork Network Controller 7.2 Device Lifecycle Management* guide.

By default, Crosswork displays the **Alarms and Events** window with the **Show** selection set to **Alarms** and the **Category** selection set to **System**, as shown below.

Figure 100: Alarms and Events window



The following table describes the main controls and features of the Alarms and Events window:

Table 67: Alarms and Events Window Controls

Item	Description	Details
1	Select alerts	Click the selection box next to the **Alarm ID** or **Event ID** column to select one or more alerts. Click the blue ID link in the **Alarm ID** or **Event ID** column to view details for that alert. On the **Alarms** window only: When you have one or more alarms selected, Crosswork enables the **Actions** menu, so you can acknowledge, clear or annotate the selected alarms.

Item	Description	Details
2	Export alerts	Click the icon to export a PDF or CSV file listing full information for all the alerts shown in the window. If you select one or more alerts when you click the icon, the file contain information only for the selected alerts.
3	Actions menu	In the **Alarms** window, click the **Actions** drop-down menu to perform one or more of these actions on the currently selected alarms: • **Acknowledge**: Marks the currently selected alarms as acknowledged. • **Unacknowledge**: If any of the currently selected alarms have been acknowledged, restores them to the unacknowledged state. • **Clear**: Removes all currently selected alarms from the **Alarms** window. • **Clear all of this condition**: Removes all currently selected alarms that share the same condition. • **Notes**: Lets you add a text note to all of the currently selected alarms. Crosswork enables the **Actions** menu only until you select one or more alarms using the selection box next to the **Alarm ID** column.
4	Toggle Alarms/Events	Toggles between the **Alarms** and **Events** windows.
5	Active Alarms only	In the **Alarms** window, select the **Active Alarms only** checkbox to display all active alarms.
6	Category selection	Click the **Category** drop-down list to select the alarm category (**System**, **Network**, or **Devices**). The default selection is **System**.
7	More Options	Click **More Options** to specify whether you want to view all alerts or only the latest, and how often to sync the alerts display with the Crosswork database. If you uncheck the **Alarm History** or **Event History** checkbox, the list shows all alerts. If you uncheck the **Auto Sync** checkbox, Crosswork pauses synchronization. **Note** In a geo HA deployment configured with dual stack, a loss of peer connectivity may cause discrepancies in the Events display flow on the standby cluster. To address the peer connectivity issue, perform the following steps: 1. Complete the application installation on the active cluster before proceeding with the installation on the standby cluster. 2. In the **Events** window on the standby cluster, click on **More options** and uncheck the **View latest events** option.
8	Saved Views	Click in the **Saved Views** field to manage the previously saved views created using the **Save View** button. In the **Manage Saved Views** window, you can view, sort, to see all views or only those you have saved.
9	Save View	Click the **Save View** button to save the current view. Crosswork will prompt you to enter and save the view under a unique name.

Item	Description	Details
10	Column Settings	Click the ⚙ to select which columns to display in the alerts list.
11	Filter	Click the ⚲ to toggle display of the floating filter fields at the top of the alerts list. You can use these fields to set filter criteria on one or more columns in the list. Click the **Filters Applied** link, shown next to the icon, to clear any filter criteria you have set.

System events

To help an operator troubleshoot issues, Crosswork Infrastructure provides a Syslog feature that forwards system-related events to an external server (see Configure a Syslog Server and *<xref to Trap Server Settings>*).

All the events related to the Crosswork platform are classified broadly into three categories: Day 0, Day 1, and Day 2.

System Event Categories and Examples

Crosswork Infrastructure system events are grouped into three main categories, each with typical actions and events.

This table lists the event categories and sample events or actions within each category:

Table 68: Event Classification and Sample Events

Event Classification	Sample Events and Actions
Day 0 – Events related only to Crosswork Infrastructure installation.	• Checking the status of the cluster • Adding a worker node • Slow disk or latency issues
Day 1 – Events related to Crosswork application installation.	• Restarting a microservice • Restarting a microservice fails • Installing an application successfully • Activating an application successfully • Application is still not healthy within 3 minutes of activation • Node drain fails • Activating an application fails • Removing a worker node

Event Classification	Sample Events and Actions
Day 2 – Events related to system operations and maintenance.	• Node eviction • Node eviction clean up fails • Deactivating an application fails/successfully • Uninstallation of an application fails/successfully • Slow disk or network • Node insertion • Node drain fails • K8S ETCD clean up • Node removal and Node removal fails

Note See the Cisco Crosswork Network Controller Supported Alarms and Events document for the complete list of supported alarms and events.

Sample day 0, day 1, and day 2 Events

Day 0, Day 1, and Day 2 events are categorized operational events in a functional system. These tables list related information to various Day 0, Day 1, and Day 2 events in a functional system

Day 0 events

These checks can help determine whether the system is healthy.

Table 69: Adding a worker node

Severity	Major
Description	A VM node has been added. This event occurs when the K8 cluster detects a node.
Sample Alarm	None
Sample Syslog Message	*<time_stamp> <hosting_hybrid_node>* *<time_stamp> <crosswork_VIP>* orchestrator-capp-infra - b54ec903-9e0f-49b8-aaf3-1d72cf644c28 vm4wkr-0 'Successfully added new VM into Inventory: vm4wkr'
Recommendation	Monitor and confirm that the VM node appears in the UI with a healthy status.

Table 70: Slow disk or latency in network issues

Severity	Critical
Description	This event occurs when the Infrastructure Capp untar takes more than 1.5 minutes or if the Docker push takes more than 2 minutes to complete. This message can be found in the firstboot.log file.
Sample Alarm	Not applicable
Sample Syslog Message	Not applicable
Recommendation	This issue must be addressed before further operations can be made on the system. Do the following: • Check that disk storage and network SLA requirements are met. • Confirm that the observed bandwidth is the same as what is provisioned between the nodes. • If using RAID, confirm it is RAID 0.

Day 1 events

These checks can help determine whether the system is healthy.

Table 71: Removing a worker node

Severity	Major
Description	This event occurs when a VM node is erased.
Sample Alarm	None
Sample Syslog Message	`<time_stamp> <hosting_hybrid_node> <time_stamp> <crosswork_VIP> CLUSTER-CLUSTER - 33a5ce0d-6cd0-4e4d-8438-85cfa8fb4ae9 CLUSTER-99 'user=admin,policyId=admin,backend=local,loginTime=2021-02-28T01:38:48Z,Category=VM Manager,RequestId=vm4wkr [Erase VM []]'`
Recommendation	Monitor and confirm that the VM node is no longer seen in the UI. If the erase operation fails, attempt to erase the node again.

Table 72: Adding an application—success

Severity	Information
Description	This event occurs when an application is added successfully.

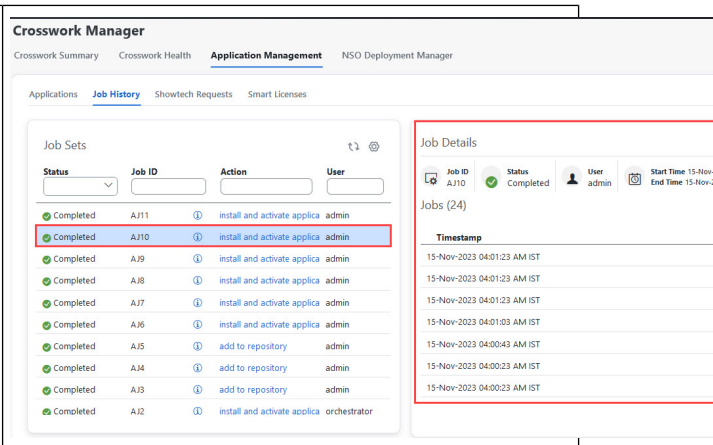
Alarm	
Syslog Message	`<time_stamp> <hosting_hybrid_node> <time_stamp> <crosswork_VIP> CLUSTER-CLUSTER - 627b2140-a906-4a96-b59b-1af22f2af9f6 CLUSTER-99 'job_type=INSTALL_AND_ACTIVATE_APPLICATION,manager=app_manager: ,user=admin,policyId=admin,backend=local,loginTime=2021-02-28T09:34:54Z,payload={"package_identifier":{"id":"cappztp","version":"1.1.0-prerelease.259+build.260"}} [accepted]'`
Recommendation	None

Table 73: Adding an application—failure

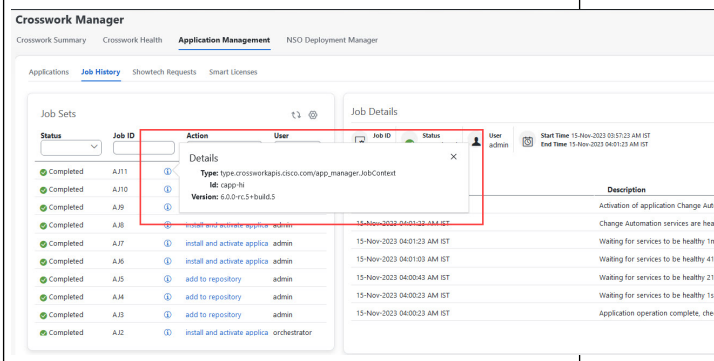
Severity	Information
Description	This event occurs when an application cannot be added.
Sample Alarm	
Sample Syslog Message	None
Recommendation	After fixing the error, try adding the application again.

Table 74: Activating an application—success

Severity	Information

Description	This event occurs after an application is activated successfully.
Sample Alarm	None
Syslog Message	`<time_stamp> <hosting_hybrid_node> <time_stamp> <crosswork_VIP> orchestrator-Crosswork Health Manager - 010689d1-8842-43c2-8ebd-5d91ded9d2d7 cw-ztp-service-0-0 ' cw-ztp-service-0 is healthy.'`
Recommendation	Activate the application and license.

Table 75: Activating an application—failure

Severity	Critical
Description	This event occurs if an application cannot be activated. The activation may fail because microservices or pods do not come up in time.
Sample Alarm	None
Syslog Message	None
Recommendation	Do the following: • Look at the job history and identify where in the activation process it failed. If it fails at the start of one of the pods coming up, restart the pods. • Uninstall the application and then try installing the application again.

Table 76: Application remains unhealthy after 3 minutes

Severity	Major
Description	This event occurs if the application was activated successfully but the components remain unhealthy after 3 minutes after application activation.
Sample Alarm	None
Sample Syslog Message	None
Recommendation	You can wait longer and if it becomes healthy, clear the alarm. Contact Cisco TAC if it still appears unhealthy after some time.

Day 2 events

Table 77: Node drain—cleanup

Severity	Information
Description	A node drain occurs if you erase a VM node or if the node has been unresponsive for more than 5 minutes. During the drain operation, pods running on the node are moved (clustered pods may move or go pending, single instance pods will move to another node).
Sample Alarms	• Node Drain Failed • K8s ETCD Cleanup Failed on Node Removal • Node Delete
Syslog Message	`<time_stamp> <hosting_hybrid_node> <time_stamp> <crosswork_VIP> orchestrator-Crosswork Health Manager - b062232f-54dc-49b2-8283-506b7bf672a6 astackserver-0-0 ' astackserver-0 health is degraded.'`
Recommendation	Monitor the operation. If the drain is a result of eviction, erase the respective node and insert a new one.

Table 78: Node drain—failure

Severity	Major
Description	A node drain occurs if you erase a VM node or if the node has been unresponsive for more than 5 minutes. This event occurs if the node drain operation fails.
Sample Alarm	None
Sample Syslog Message	`<time_stamp> <hosting_hybrid_node> <time_stamp> <crosswork_VIP> orchestrator-Crosswork Health Manager - b062232f-54dc-49b2-8283-506b7bf672a6 astackserver-0-0 ' astackserver-0 health is degraded.'`
Recommendation	Try erasing the node again.

Table 79: Node eviction—failure

Severity	Critical

Description	In this scenario we assume that one of the hybrid nodes fails. This event occurs if the node has been down for more than 5 minutes and it is automatically taken out of service. This event can be triggered if someone stopped or deleted a VM without using Cisco Crosswork or if there is a network outage to that node. K8s automatically start evicting pods on that node (drain eviction operation). The VM node will be marked down during a successful cleanup.
Sample Alarm	• Node Eviction Cleanup Failure • K8S ETCD Cleanup Failed on Node Removal
Syslog Message	None
Recommendation	Erase the faulty node and insert a new VM.

Table 80: Node eviction—cleanup failure

Severity	Critical
Description	This event occurs when the drain eviction fails. The node has been down for more than 5 minutes and K8s automatically start evicting pods on that node.
Sample Alarm	None
Sample Syslog Message	None
Recommendation	Erase the node and attempt another cleanup operation.

Table 81: Resource footprint shortage

Severity	Critical
Description	This event occurs when cluster node resources are being highly utilized and there is a lack of a resource footprint.
Sample Alarm	None
Sample Syslog Message	None
Recommendation	Add a new worker node.

Table 82: Deactivating an application—success

Severity	Minor

Description	This event occurs when an application is deactivated.
Sample Alarm	None
Sample Syslog Message	*<time_stamp> <hosting_hybrid_node>* *<time_stamp> <crosswork_VIP>* CLUSTER-CLUSTER - ade982ea-7f60-4d6b-b7e0-ebafc789edee CLUSTER-99 © 2021 Cisco and/or its affiliates. All rights reserved. Cisco Confidential – DRAFT version 1 'user=admin,policyId=admin,backend=local,loginTime=2021-02-28T09:34:54Z,job_type=UNINSTALL_APPLICATION,manager=app_manager:,payload={"application_id":"capp-ztp"} [accepted]'
Recommendation	None

Table 83: Deactivating an application—failure

Severity	Critical
Description	This event occurs when an application cannot be deactivated. This can occu if microservices or pods are still running.
Sample Alarm	None
Syslog Message	None
Recommendation	Do the following: • Look at the job history and identify where in the activation process it failed. If it fails at the start of one of the pods coming up, restart the pods. • Uninstall the application and then try installing the application again.

Table 84: Slow disk or latency in network issues

Severity	Critical
Description	This event occurs when the Infrastructure Capp untar takes more than 1.5 minutes or if the Docker push takes more than 2 minutes to complete. This message can be found in the firstboot.log file.
Sample Alarm	Not applicable
Sample Syslog Message	Not applicable

Recommendation	This issue must be addressed before further operations can be made on the system. Do the following: • Check that disk storage and network SLA requirements are met. • Confirm that the observed bandwidth is the same as what is provisioned between the nodes. • If using RAID, confirm it is RAID 0.

Note There a one-time check performed to ensure the hardware attempts to meet the Disk SLA. If this fails, a critical alarm is issued. User can address the alarm as needed and manually clear the alarm.

Table 85: ETCD cleanup

Severity	Information
Description	This event occurs if someone erases a VM node and the ETCD clean membership cleanup operation begins.
Sample Alarms	If ETCD cleanup fails: • K8S ETCD Cleanup Failed on Node Removal • Alarm Node Delete
Syslog Message	None
Recommendation	Monitor operation.

Table 86: K8S ETCD cleanup failed on node removal

Severity	Major
Description	This event occurs if the ETCD cleanup operation fails.
Sample Alarm	None
Sample Syslog Message	None
Recommendation	Try erasing the node again.

Table 87: Restart microservices—failure

Severity	Warning
Description	This event occurs when someone restarts a microservice or pod and the operation fails.

Sample Alarm	None
Sample Syslog Message	None
Recommendation	Restart the microservices or pods. You may have to do this a few times to see if it recovers.

Enable trap handling

In addition to UI options, REST APIs, and Syslogs, Cisco Crosswork allows users to generate SNMP traps for events and alarms to notify the application and cluster health.

- Supports SNMPv2 and SNMPv3 protocols for sending traps.
- Alarms and events are filtered based on user-defined criteria before being converted to traps.
- Traps are sent to the trap server using the alarm model in CISCO-EPM-NOTIFICATION-MIB.

For configuration details, see <*xref to Trap server settings*>.

For more information on the alarm model, see Cisco EPM Notification MIB.

Collect audit information

Audit logs are records that map user information with all critical user actions performed in the system.

- Audit logs capture user actions across these core platform areas:
  - *User and system administration:* device onboarding, user creation/deletion/configuration updates, dashboard customization, show-tech execution, and topology/grouping operations.
  - *Data and operational management:* backup/restore, Crosswork Data Gateway, Inventory (manual sync, enable/disable RI, export, Resync API), and performance policy CRUD and health settings updates.
  - *Automation and orchestration:* Change Automation actions (playbooks, KPIs, KPI Profiles, Alert groups).
  - *Network optimization and provisioning:* Optimization Engine operations (SR-TE, RSVP-TE, affinity mapping, bandwidth functions, RESTCONF operations).
- Audit logs capture the source IP for all logged operations. This includes:
  - *Infrastructure services:* TLS certificate operations, app and FP package actions, Placement/Node/Cluster Manager APIs, GEO & Cross-cluster Manager APIs, DLM CRUD actions, performance configuration changes, topology/grouping operations, and dg-manager CRUD (HA pools, custom packages, resource updates, destinations).
  - *Telemetry and data-collection services:* Helios collection job actions, Health Insight API operations, NPM monitoring and data-retention updates, CLMS registration/de-registration/transport settings, and CAT-FP deployment CRUD.

- *Provisioning and NSO-routed operations:* all CRUD in ZTP (serial numbers, vouchers, profiles, devices), all Image Service operations (with user name and source IP), EMS Inventory APIs, and all NSO JSON-RPC/RESTCONF requests routed through cw-proxy.

- Audit logs capture creation of collection jobs and related behaviors, including per-device entries when applicable, and exclude events triggered automatically by internal services.

User actions captured in audit logs

The audit log includes user actions related to these operations:

- Device onboarding
- User creation, deletion, and configuration updates
- Crosswork Data Gateway management operations
- Collection job creation
- Administrative tasks (show-tech execution, topology updates, NSO-related actions)
- Manage playbooks (import, export, delete) and playbook execution, including logs for execution requests, maintenance tasks, execution IDs, and commit labels

Note When a playbook execution request is sent, Change Automation prints an audit log. The audit log includes details like the playbook name, user information, session details, and the execution ID of the job. When Change Automation executes a playbook maintenance task, it also prints an audit log. The maintenance audit log contains details such as the execution ID. If it performs the commit on NSO, the maintenance audit log details also include the commit label. You can use the audit log to identify all the commit labels associated with an execution ID. Use the commit labels to perform a lookup on the NCS CLI. The lookup shows the exact configuration changes that Change Automation pushed to the device.

- KPIs, KPI Profiles, and Alert group creation, deletion, configuration updates, and enabling or disabling of KPI Profiles
- Crosswork Optimization Engine operations such as SR-TE and RSVP-TE tunnel management, affinity mapping, bandwidth functions, and RESTCONF operations

Sample audit log entry

This sample log includes source IP, username, and operation details implemented in this release.

```
2025-10-23T21:03:05.230Z 10.194.126.46 CW[Proxy] 0000019a-12e1-e40e-0000-019a12e1e40e
AUDITLOG-CW Proxy-1761253385230-AUDIT_LOG 'CW Proxy -- Attempted commit with transaction
id 2 -- N/A --  -- rwonly -- 172.22.227.147'
2025-10-23T21:03:48.516Z 10.194.126.46 AAA 0000019a-12e2-8d24-0000-019a12e28d24
AUDITLOG-AAA-1761253428516-AUDIT_LOG 'AAA -- Login successful -- N/A --  -- localadmin --
172.22.227.147'
```

This sample audit log entry is created when a local admin user runs a playbook.

```
time="2026-01-09 21:24:31.103312" level=info msg="playbook scheduled for execution"
backend=local execution_id=1591737871096-a6699d03-8264-4ea8-8f6f-03e8a58f32a3
latency=11.330355ms loginTime="2026-01-09T20:27:11Z" method=POST
playbook="router_config_traffic_steering" policyId=admin
set_id=5405fdb1-6b37-41cb-94a3-32b180d3b773 set_name=static-acl-b180d3b773
tag="ROBOT_manager-nca-7689b-fdn8g" user=admin
```

This is a Crosswork Optimization Engine RESTCONF API audit log entry sample:

```
time="2026-01-06 13:49:06,308"
message="action=/operations/cisco-crosswork-optimization-engine-sr-policy-operations:sr-policy-delete,
 input={\"input\": {\"sr-policies\": [{\"head-end\": \"192.168.0.2\", \"end-point\":
\"192.168.0.3\", \"color\": 301}]}},
output={\"cisco-crosswork-optimization-engine-sr-policy-operations:output\":{\"results\":
[{\"head-end\":\"192.168.0.2\",\"end-point\":\"192.168.0.3\",\"color\":301, \"message\":\"SR
 policy  not found in Config DB\",\"state\":\"failure\"}]}}" user=admin policyId=admin
backend=local loginTime=1591451346 method=POST
url=/operations/cisco-crosswork-optimization-engine-sr-policy-operations:sr-policy-delete
```

Common audit log entry fields

Table 88: Common Audit Log Entry Fields

Field	Description
time	The time that Crosswork created this audit log.
message	Message sent between applications.
msg	Message sent between applications.
user	Name of the user.
policyId	Role or permission of user (taken from local database, TACACS, or LDAP server).
backend	The server (local database, TACACS, or LDAP) authenticating users.
loginTime	The epoch time when the user has logged in. Epoch time is intentionally selected, as it is shorter and independent of time zones.
Other fields	Individual applications use more fields specific to that application. For example: • In the sample audit log entry for Cisco Crosswork Change Automation and Health Insights, the **playbook** field refers to the playbook that Change Automation executed. • In the UI audit log entry for Crosswork Optimization Engine, **data** is a field that refers to the creation details of an SR-TE policy and its attributes.

Audit log location

Crosswork stores audit logs in `/var/log/audit/audit.log`, under the respective application pods. For example:

- The sample Change Automation audit log is in the `<robot-nca>` data directory under the pod.
- The RESTCONF API audit log is under the `optima-restconf` pod.

In addition to the individual application audit logs, Cisco Crosswork collects all audit log files once each hour. Crosswork stores them as separate gzipped tar files in this data directory:
`/mnt/robot_datafs/<app-name>/<instance>/auditlogs/auditlogs.tar.gz`

Crosswork collects audit log files based on the specified maximum size and number of backups for each application. For example: **`MaxSize:20 megabytes`** and **`MaxBackups: 5`**.

View Audit Log

The **Audit Log** window tracks the following AAA-related events:

- Create, update, and delete users
- Create, update, and delete roles
- User login activites - login, logout, login failure due to maximum active session limit, and account locked due to maximum login failures.
- Source IP - IP address of the machine from where the action was performed. This column appears only when you check the **Enable source IP for auditing** check box and relogin to Cisco Crosswork. This check box is available in the **Source IP** section of the **Administration** > **AAA** > **Settings** page.
- Password modification by user

To view the audit log, perform the following steps:

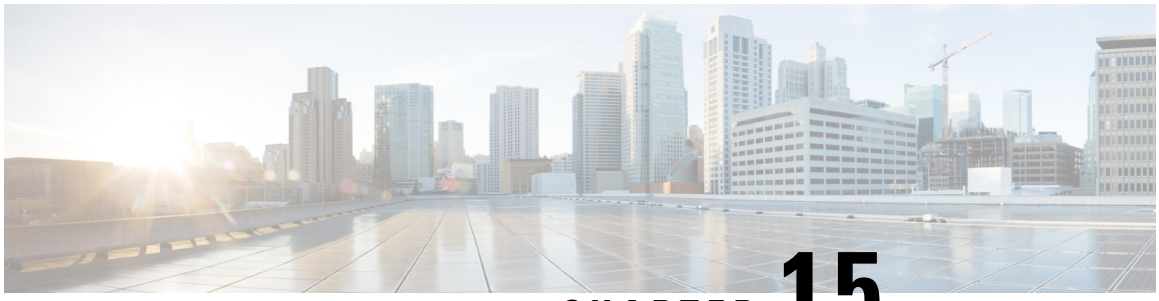
Procedure

Step 1 From the main menu, choose **Administration** > **Audit Log**.

The **Audit Log** window is displayed.

Step 2 Click ⏷ to filter the results based on your query.

Using the export icon, you can export the log in the CSV format. When exporting the CSV, you have the option to use the default file name or enter a unique name.



CHAPTER 15

Manage Crosswork Data Gateway Base VM

A Crosswork Data Gateway instance is deployed as a standalone entity. It can be located in a different geographic region than the controller application, such as Crosswork Cloud or Crosswork Network Controller.

This instance connects to the controller application and enables seamless data collection from the network.

This chapter covers these topics.

Crosswork Data Gateway interactive console

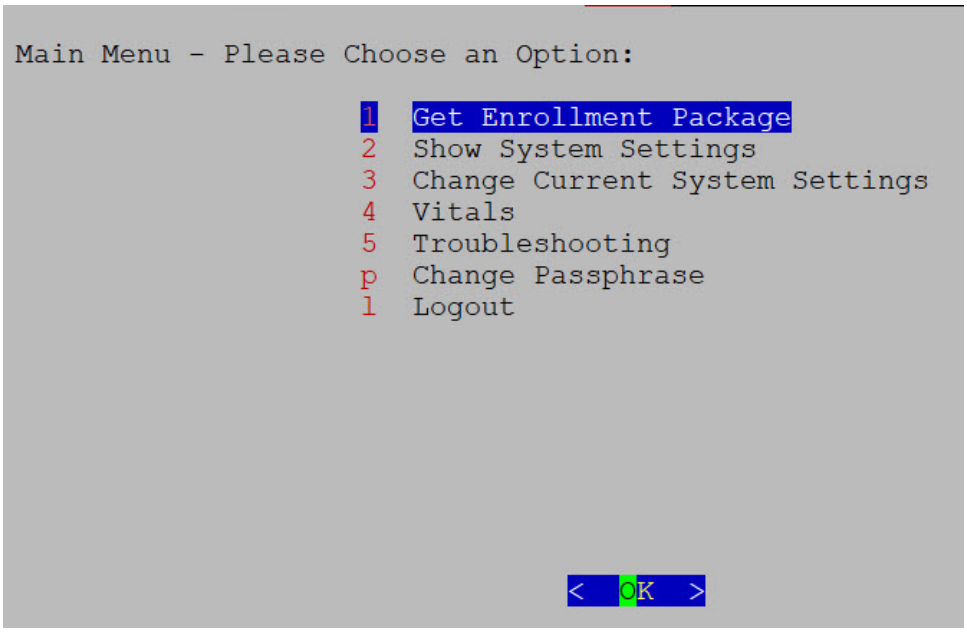
When you log in to the Crosswork Data Gateway, an interactive console is launched. It provides a command-line interface for managing and troubleshooting the system.

The console presents a main menu upon successful login.

Main menu overview and role-based access

The main menu displays various options based on the user's role and privileges. Options differ for the **Administrator** (dg-admin) and the **Operator** (dg-oper) roles. Here is an example of the main menu as seen by the **dg-admin** user:

Figure 101: Interactive console



The main menu presents these options:

- Get Enrollment Package
- Show System Settings
- Change Current System Settings
- Vitals
- Troubleshooting
- Change Passphrase
- Log out

User roles and configuration guidelines

- The main menu for the **dg-oper** user differs, as the operator has more limited access compared to the administrator. Refer to the Role-based permissions table for a detailed breakdown of user roles and their associated privileges.
- When using an IPv6 address for any configuration, enclose it in square brackets, as in ([1::1]).

Manage Crosswork Data Gateway users

This section contains these topics:

- Supported user roles, on page 479
- Change the user passphrase, on page 481

Supported user roles

Crosswork Data Gateway supports two default user roles. Each role has specific permissions and responsibilities.

- **Administrator role**:
  - **Username**: `dg-admin`
  - **Description**: This user is created by default when Crosswork Data Gateway is set up for the first time. The `dg-admin` user has full administrative privileges, which include both read and write access.

    Permissions:
    - Starting and shutting down the Crosswork Data Gateway VM.
    - Registering applications within the system.
    - Applying authentication certificates.
    - Configuring server settings.
    - Performing kernel upgrades.

      For other permissions, see Role-based permissions.

    Note that the `dg-admin` user cannot be deleted.

- **Operator role**: The **dg-oper** user is also created by default during the initial VM startup. This user can review the health of the Crosswork Data Gateway, retrieve error logs, receive error notifications, and run connectivity tests between the Crosswork Data Gateway instance and the output destination.
  - **Username**: `dg-oper`
  - **Description**: This user is also created by default during the initial deployment of the Crosswork Data Gateway VM. The `dg-oper` user has a more limited set of permissions, focusing on system monitoring and troubleshooting.
  - **Permissions**:
    - Reviewing the health status of Crosswork Data Gateway.
    - Retrieving error logs.
    - Receiving error notifications.
    - Running connectivity tests between the Crosswork Data Gateway instance and its output destination.

      For other permissions, see Role-based permissions.

Role-based permissions for administrators and operators

Table 89: Role-based permissions

Permissions	Administrator	Operator
Get Enrollment Package	✓	✓

Permissions	Administrator	Operator
Show system settings		
vNIC Addresses NTP DNS Proxy UUID Syslog Certificates First Boot Provisioning Log Timezone	✓	✓
Change Current System Settings		
Configure NTP Configure DNS Configure Control Proxy Configure Static Routes Configure Syslog Create new SSH keys Import Certificate Configure vNIC MTU Configure Timezone Configure Password Requirements Configure Simultaneous Login Limits Configure Idle Timeout Configure Login Check Frequency Configure Interface Address	✓	×
Vitals		

Permissions	Administrator	Operator
Docker Containers Docker Images Controller Reachability NTP Reachability Route Table ARP Table Network Connections Disk Space Usage Linux services NTP Status System Uptime	✓	✓
Troubleshooting		
Run Diagnostic Commands	✓	✓
Run show-tech	✓	✓
Remove All Non-Infra Containers and Reboot VM	✓	×
Reboot VM	✓	×
Export audited logs	✓	✓
Re-enroll Data Gateway	✓	✓
Enable TAC Shell Access	✓	×
Change Passphrase	✓	✓

User authentication

- Both the `dg-admin` and `dg-oper` accounts are configured with credentials during the installation of Crosswork Data Gateway.
- User authentication is local to the system. Authentication occurs within the system rather than through an external identity provider.

Change the user passphrase

Both **Administrator** and **Operator** users can change their own passphrases, but they cannot change each other's passphrases.

To change your passphrase, use these steps:

Procedure

Step 1 From the Main Menu, select **Change Passphrase** and click **OK**.

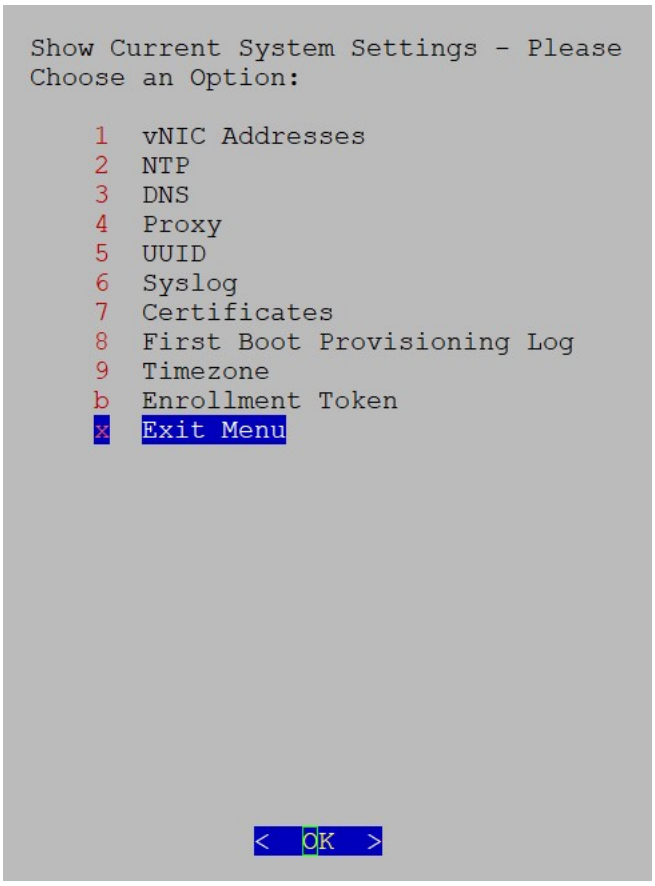
Step 2 Enter your **current password**, then press **Enter**.

Step 3 Enter your **new password** and press **Enter**. To confirm, re-type your **new password** and press **Enter**.

View the system settings

You can view various system settings through Crosswork Data Gateway.

Figure 102: Show current system settings menu



Complete these steps to view the current system configuration.

Procedure

Step 1 From the Main Menu, select **Show System Settings**.

Step 2 In the prompt, click **OK** to open the **Show Current System Settings** menu.

Step 3 Select the setting that you want to view.

Setting option	Description
vNIC Addresses	Displays the vNIC configuration, including address information.
NTP	Displays the details of the currently configured Network Time Protocol (NTP) server.
DNS	Displays the details of the Domain Name System (DNS) server configuration.
Proxy	Displays the proxy server details (if any proxy is configured).
UUID	Displays the system UUID.
Syslog	Displays the syslog forwarding configuration. If the forwarding configuration is not set, only the message "# Forwarding configuration follows" is displayed.
Certificates	You can view certificate files such as: • Crosswork Data Gateway signing certificate file • controller signing certificate file • controller SSL/TLS certificate file • syslog certificate, and • collector certificate.
First Boot Provisioning Log	Displays the content of the first boot log file.
Timezone	Displays the current timezone setting.
Enrollment Token	**Attention** This menu option is for users of Crosswork Data Gateway for Cloud applications. Displays the token that is used by Crosswork Data Gateway to enroll with Crosswork Cloud.

Change the system settings

Crosswork Data Gateway allows you to configure various system settings. The **Change Current System Settings** menu provides access to these options.

Follow these steps to modify the current system settings:

Before you begin

Ensure you are aware of these considerations and requirements:

- **Enrollment token**: The **Enrollment Token** menu option is intended for users of **Crosswork Data Gateway for Cloud** applications.
- **Administrator access**: Only the administrator can modify system settings.
- **IPv6 address format**: When you use an IPv6 address, enclose it in square brackets (for example, `[1::1]`).
- **SCP port configuration**: If you need to use a custom SCP port (not the default port 22), specify the port in the SCP command with the syntax:

  ```
  -P55
                                  user@host:path/to/file
  ```

  In this example, **55** is the custom port number.

Procedure

Step 1 From the Main Menu, select **3 Change Current System Settings**.

Step 2 Select the setting that you want to modify.

Configure the NTP time

It is essential for the NTP time to be synchronized between the controller application and its Crosswork Data Gateway instances.

If the time is not synchronized, session handshakes fail, and functional images will not be downloaded. In such cases, the following error message will be logged in the controller-gateway.log: Clock time not matched and sync failed.

How to access the log files

Use the **Run show-tech** command. For more information, see Run the Showtech Command. You can check the NTP reachability for both the controller application and Crosswork Data Gateway by using the **Controller Reachability** and **NTP Reachability** options from the **Main Menu** > **Vitals**. For more information, see View the Crosswork Data Gateway vitals.

If NTP is incorrectly configured, the error **Session not established** will appear.

Key considerations for NTP configuration

- When configuring **Crosswork Data Gateway** to use authentication via a keys file, the **chrony.keys** file must follow the specific format that is documented at chrony.conf documentation.
- For sites using **ntpd** and a **ntp.keys** file, you can convert the **ntp.keys** to a **chrony.keys** file using the conversion tool available at ntp2chrony tool.

  This tool converts the **ntpd** configuration into a **chrony** compatible format, but only the **keys file** is needed for importing into Crosswork Data Gateway.

Follow the steps to configure NTP settings:

Procedure

Step 1 From the **Change Current System Settings** menu, select **Configure NTP**.

Step 2 Enter the details for the new NTP server:

- Server list with each server separated by a space
- Use NTP authentication?
- Key list, with each key separated by a space, and the number of keys must match the number of servers in the list
- Key file passphrase to use Secure Copy Protocol (SCP) to the VM
- Key file passphrase to SCP to the VM

Step 3 Click **OK** to save the settings.

Configure the DNS

By configuring DNS in Crosswork Network Controller, users can enable the system to resolve hostnames to IP addresses, ensuring reliable communication with external servers and services. This setup is essential for seamless integration, software updates, and connectivity to various network resources.

To configure DNS settings for Crosswork Data Gateway, use these steps:

Procedure

Step 1 From the **Change Current System Settings** menu, select **Configure DNS** and click **OK**.

Step 2 Enter the new DNS server addresses and domain.

Step 3 Click **OK** to save the settings.

Configure the control proxy

If a proxy server was not configured during the installation, you can set up the proxy server using this option.

Procedure

Step 1 From the **Change Current System Settings** menu, select **Configure Control Proxy** and click **OK**.

Step 2 In the confirmation dialog, click **Yes** to proceed. Click **Cancel** if you do not wish to proceed.

Step 3 Enter the following **Proxy server** details:

- server URL,
- bypass addresses,
- proxy username, and
- proxy passphrase.

Step 4 Click **OK** to save the settings.

Configure static routes

Static routes are typically configured when Crosswork Data Gateway receives addition or deletion requests from the collectors. The **Configure Static Routes** option from the main menu can also be used for troubleshooting purposes.

Caution Static routes configured using this option are lost when the Crosswork Data Gateway reboots.

Add the static routes

Before you begin

To add a static route, complete the steps.

Procedure

Step 1 From the **Change Current System Settings** menu, select **4 Configure Static Routes**.

Step 2 To add a static route, select **Add**.

Step 3 Select the interface for which you want to add a static route.

Step 4 Select the **IP version**.

Step 5 Enter the **IPv4** or **IPv6 subnet** in CIDR format when prompted.

Step 6 Click **OK** to save the settings.

Delete the static routes

Before you begin

To delete a static route, complete the steps.

Procedure

Step 1 From the **Change Current System Settings** menu, select **4 Configure Static Routes**.
Step 2 To delete a static route, select **Delete**.
Step 3 Select the interface for which you want to delete a static route.
Step 4 Select the **IP version**.
Step 5 Enter the **IPv4** or **IPv6 subnet** in CIDR format.
Step 6 Click **OK** to save the settings.

Configure the syslog system

The syslog server can be configured during Day0 installation through the configuration file. If you wish to modify the syslog server list, port number, protocol, or certificate file later (Day1 or beyond), you can use the Interactive Console.

Note For syslog server configuration with IPv4 or IPv6 support on different Linux distributions, refer to your system administrator and configuration guides.

Syslog configuration modes:

- **Simultaneous**: Crosswork Data Gateway sends messages to all the configured syslog server addresses. If one of the servers is unresponsive, the message is queued to the disk until the servers respond.
- **Failover**: Crosswork Data Gateway sends messages to the first syslog server address. If the server is unavailable, the message is sent to the subsequent configured address. If all servers are unresponsive, the message is queued to the disk until a server responds.

To configure syslog, complete these steps.

Procedure

Step 1 From the **Change Current System Settings** menu, select **5 Configure Syslog**.
Step 2 In the **Use Syslog** window, select **True** to continue configuring the syslog server.
Step 3 In the **Select Syslog Multiserver Mode** window, select either **Simultaneous** or **Failover**.
Step 4 Enter the values for the following syslog attributes:

- **Server address or hostname**: Enter a space-delimited list of IPv4 or IPv6 addresses for one or more syslog servers that are accessible from the management interface.
- **Port**: Enter the port number of the syslog server.
- **Protocol**: Choose **UDP**, **TCP**, or **RELP** for sending system logs.

- **Use Syslog over TLS?**: To encrypt syslog traffic using TLS, select **Yes**.
- **TLS Peer Name**: Enter the syslog server's hostname as it appears in the server certificate **SubjectAltName** or **Subject Common Name**.
- **Syslog Root Certificate File URI**: Enter the URI for the PEM-formatted root certificate of the syslog server, which is retrieved using SCP.
- **Syslog Certificate File Passphrase**: Enter the password for the SCP user to retrieve the syslog certificate chain.

Step 5 Click **OK** to save the settings.

Create the new SSH keys

Creating new SSH keys overwrites the current keys.

To create new SSH keys, follow these steps.

Procedure

Step 1 From the **Change Current System Settings** menu, select **6 Create new SSH keys**.

Step 2 Click **OK**.

Crosswork Data Gateway launches an auto-configuration process that generates new SSH keys.

Import a certificate

If you update any certificate except the **Controller Signing Certificate**, the collector restarts.

Crosswork Data Gateway allows you to import these certificates:

- Controller signing certificate file
- Controller SSL or TLS certificate file
- Syslog certificate file
- Proxy certificate file

Procedure

Step 1 From the **Change Current System Settings** menu, select **Import Certificate**.

Step 2 Select the certificate you want to import.

Step 3 Enter the **SCP URI** for the selected certificate file.

Step 4 Enter the **passphrase** for the SCP URI and click **OK**.

Configure the vNIC2 MTU

You can modify the **vNIC2 MTU** only if you are using 3 NICs and:

- If your interface supports jumbo frames, the valid MTU range is 60 to 9000.
- If the interface does not support jumbo frames, the valid MTU range is 60 to 1500.

Setting an invalid MTU causes Crosswork Data Gateway to revert to the currently configured value. Ensure that the MTU value is within the supported range as specified in your hardware documentation. Errors related to MTU changes are logged in **kern.log** and can be viewed after running **showtech**.

Procedure

Step 1 From the **Change Current System Settings** menu, select **Configure vNIC2 MTU**.
Step 2 Enter the desired **vNIC2 MTU** value.
Step 3 Click **OK** to save the settings.

Configure the timezone of the Crosswork Data Gateway VM

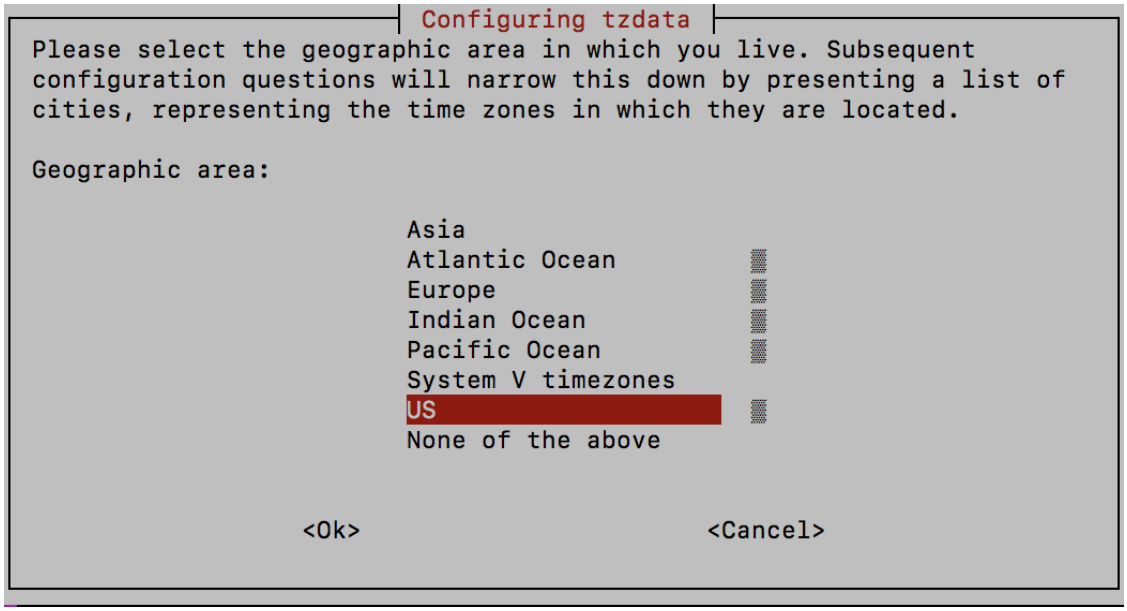
By default, the Crosswork Data Gateway VM launches with the UTC timezone.

Update the timezone so that all Data Gateway processes, including Showtech logs, reflect the correct timestamp for your location.

Procedure

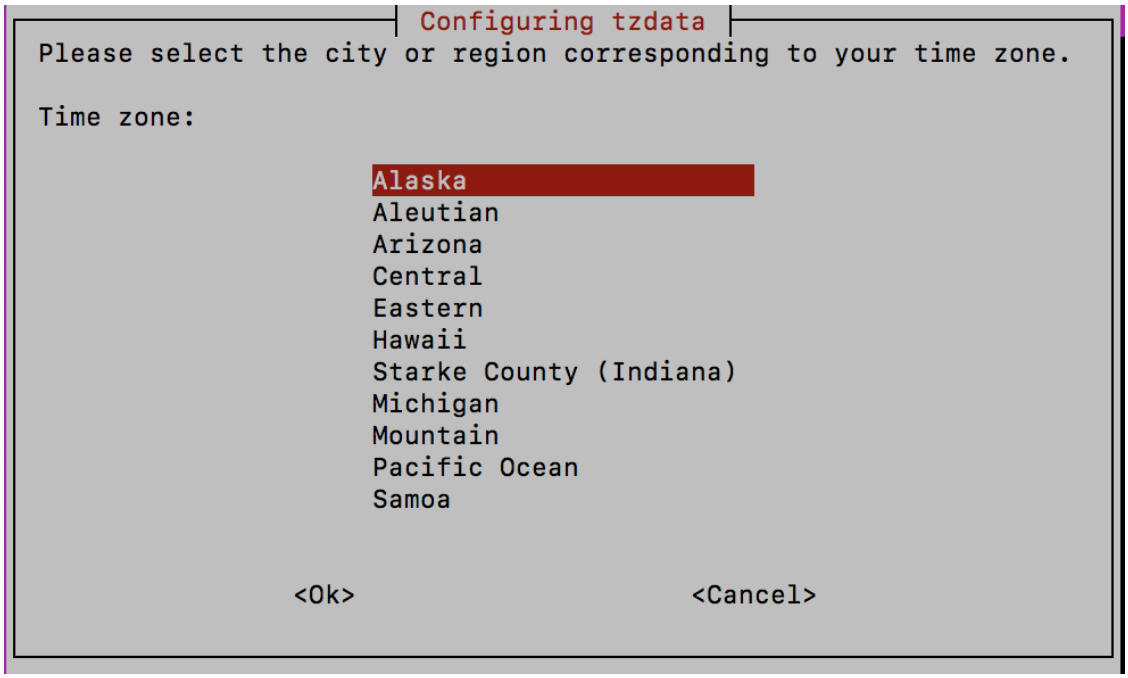
Step 1 Log in to the Crosswork Data Gateway VM.
Step 2 Select **3 Change Current System Settings** in the Crosswork Data Gateway VM interactive menu.
Step 3 Select **9 Timezone** from the menu.
Step 4 Select the geographical area in which you are located.

Figure 103: Geographic area selection



Step 5 Select the city or region that corresponds to your timezone.

Figure 104: Region selection



Step 6 Select **OK** to save the settings.

Step 7 Reboot the Crosswork Data Gateway VM to apply the new timezone to all processes.

Step 8 Log out of the Crosswork Data Gateway VM.

Configure the password requirements

You can configure various password requirements, including:

- Password strength
- Password history
- Password expiration

and

- Login failures

Procedure

Step 1 From the **Change Current System Settings** menu, select **Configure Password Requirements**.

Step 2 Select the password requirement you want to change.

Set the options for the selected requirement:

- **Password strength**
- **Password history**
- **Password expiration**
- **Login Failures**

Step 3 Click **OK** to save the settings.

Configure the simultaneous login limits

By default, Crosswork Data Gateway supports ten simultaneous sessions for the **dg-admin** and **dg-oper** users on each VM. To change this limit, use these steps:

Procedure

Step 1 From the **Change Current System Settings** menu, select **Configure Simultaneous Login Limits**.

Step 2 In the window that appears, enter the desired number of simultaneous sessions for the **dg-admin** and **dg-oper** users.

Step 3 Click **OK** to save your changes.

Configure an idle timeout

After a specified idle timeout, the system will automatically log out any inactive user session.

Procedure

Step 1 From the **Change Current System Settings** menu, select **b Configure Idle Timeout**.

Step 2 Enter the desired idle timeout value in the window that appears.

Step 3 Enter **OK** to save your changes.

Configure a remote auditd server

To export logs to a remote **auditd** server, perform the steps in this procedure.

Procedure

Step 1 From the **Change Current System Settings** menu, select **c Configure Auditd**.

Step 2 Enter the following details.

- Remote auditd server address.
- Remote auditd server port.

Step 3 Select **OK** to save your changes.

Configure the login check frequency

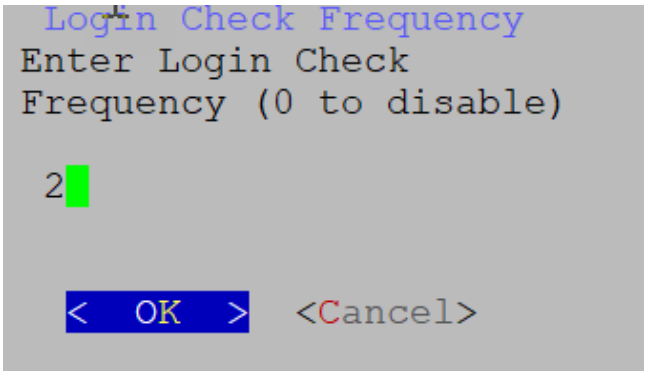
You can configure the number of permissible login attempts allowed after a failed login. If you want to disable the feature, set the frequency to zero.

Procedure

Step 1 From the **Change Current System Settings** menu, select **Configure Login Check Frequency** and click **OK**.

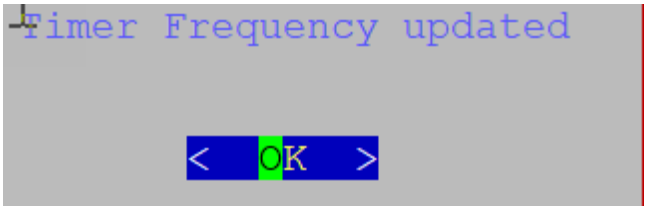
Step 2 In the **Login Check Frequency** window, enter the number of login attempts you want to allow after a failure. To disable the feature, enter **0**.

Figure 105: Login check frequency



After the timer is updated, a confirmation window appears.

Figure 106: Timer frequency



Configure an interface address

After deploying a Crosswork Data Gateway instance, you can reconfigure the network interfaces that are associated with it. The reconfiguration allows you to modify an interface's name, IP address, or security group association.

Before you begin

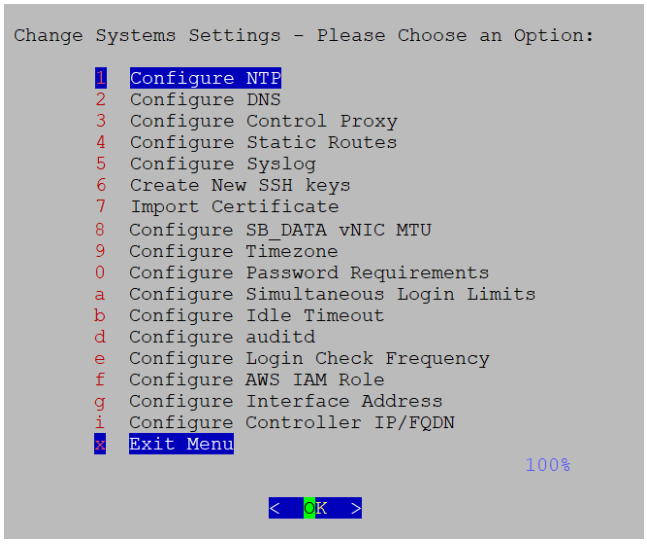
Before reconfiguring the interface address, make sure to:

- Ensure that all devices are detached from the Crosswork Data Gateway instance.
- Verify that the Crosswork Data Gateway instance is in maintenance mode.

Procedure

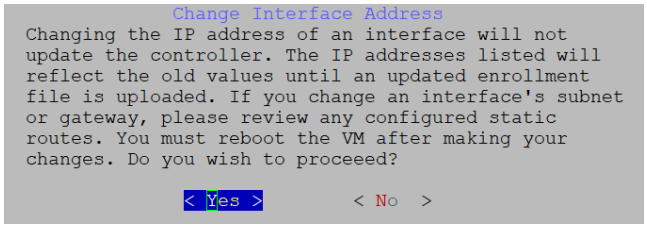
Step 1 From the **Change System Settings** menu, select **Configure Interface Address**.

Figure 107: System settings



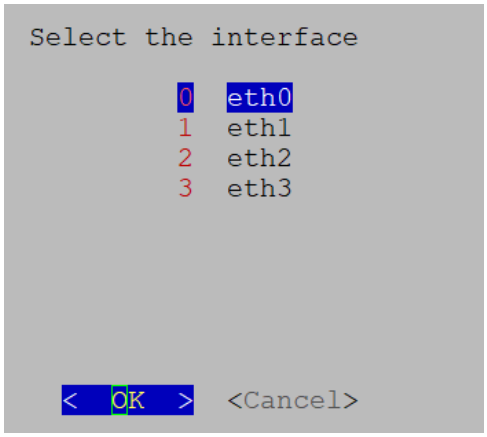
Step 2 In the **Change Interface Address** confirmation box, click **Yes**.

Figure 108: Change interface address confirmation message



Step 3 Select the interface that you want to reconfigure with options are `eth0` , `eth1`, `eth2`, or `eth3`. Click **OK**.

Figure 109: Interface selection



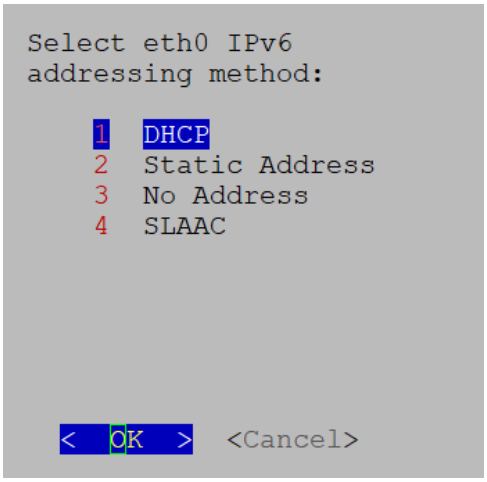
Step 4 Choose the IPv4 addressing method for the interface. You can select from:

- DHCP

- Static Address
- No address

Note
Cisco recommends that you select the option you configured during the **Day0** installation.

Figure 110: IPv6 address selection



Step 5 Enter the IPv4:

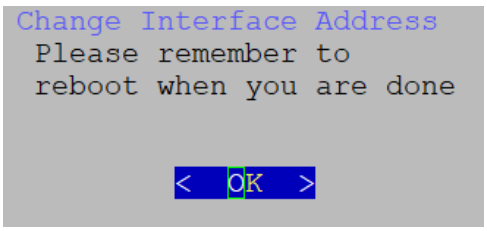
- address and click **OK**.
- netmask address and click **OK**.

Step 6 In the **Skip Interface IPv4 Gateway Configuration** confirmation box, select **True** or **False** and click **OK**.

Step 7 If you selected **True** in the previous step, specify the **IPv4 gateway address**.

Step 8 In the **Change Interface Address** confirmation box, click **OK**.

Figure 111: Confirmation message



Step 9 After reconfiguring the interface, reboot the VM to apply the changes.

Configure the controller IP for Crosswork Data Gateway

This topic explains the procedure for configuring the Controller IP or fully qualified domain name (FQDN) for the Crosswork Data Gateway after enabling the Geo Redundancy feature.

When a Data Gateway is deployed with an invalid Controller IP, it may get stuck in the enrollment process. To address this, reconfigure the Controller IP. Also, if a Data Gateway is enrolled to a Crosswork and there is a change in Controller virtual IP address (VIP IP) or the IP is changed to FQDN due to the enabled Geo Redundancy feature, it needs to be reconfigured.

To configure the controller IP for a new enrollment or change the controller IP of an existing Crosswork that the Data Gateway is enrolled with:

Navigate to the Data Gateway on the active cluster before the geo redundancy feature is enabled.

Procedure

Step 1 From the **Change Current System Settings** menu, select **Configure Controller IP/FQDN**

Step 2 Enter the SCP URI for the controller signing certificate file.

Step 3 Enter the SCP passphrase or the SCP user password for the controller-signing certificate file.

Step 4 Enter the IP address for the controller.

A message appears to confirm that Crosswork has updated the IP address or FQDN of the controller, and the VM is rebooted.

View the Crosswork Data Gateway vitals

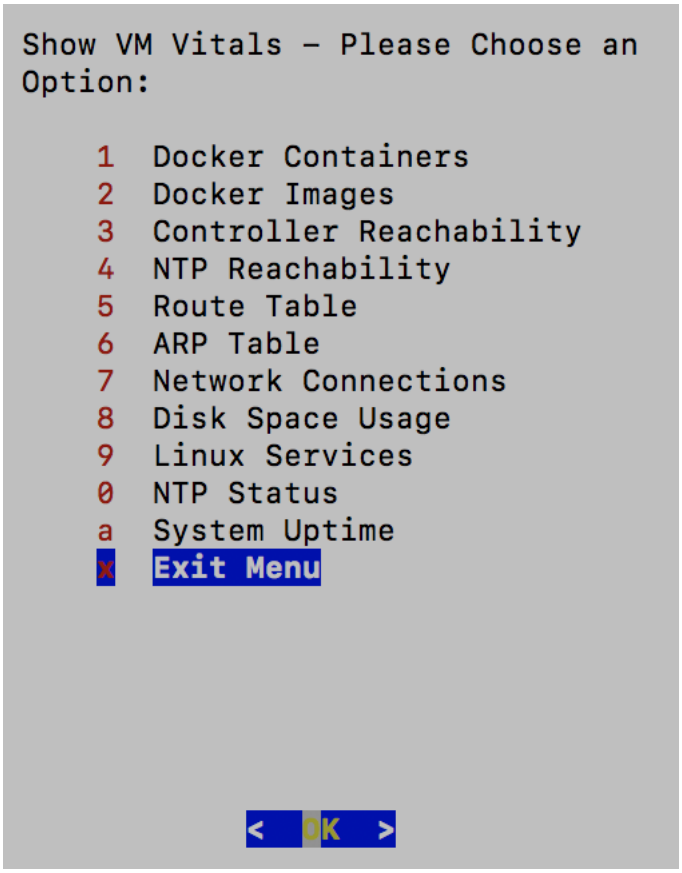
To view Crosswork Data Gateway vitals, use these steps.

Procedure

Step 1 From the Main Menu, select **Vitals**.

Step 2 From the **Show VM Vitals** menu, select the vital you want to view.

Figure 112: Show the VM vitals



Vital	Description
Docker Containers	The system displays the following vitals for the Docker containers currently instantiated in the system. • Container ID • Image • Name • Command • Created Time • Status • Port

Vital	Description
Docker Images	The system displays the following details for the Docker images currently saved in the system. • Repository • Image ID • Created Time • Size • Tag
Controller Reachability	The system displays the results of the controller reachability test run. • Default IPv4 gateway • Default IPv6 gateway • DNS server • Controller • Controller session status
NTP Reachability	The system displays the results of NTP reachability tests. • NTP server resolution • Ping • NTP Status • Current system time
Route Table	The system displays the IPv4 and IPv6 routing tables.
ARP Table	The system displays the ARP tables.
Network Connections	The system displays the current network connections and listening ports.
Disk Space Usage	The system displays the current disk space usage for all partitions.
Linux Services	The system displays the status of these Linux services. • NTP • SSH • Syslog • Docker • Crosswork Data Gateway Infrastructure containers.
Check NTP Status	The system displays the NTP server status.

Vital	Description
Check System Uptime	The system displays the system uptime.

Crosswork Data Gateway VMs troubleshooting

To access the **Troubleshooting** menu, select **5 Troubleshooting** from the **Main Menu**.

Troubleshooting menu overview

The **Troubleshooting** menu provides several options to diagnose and resolve issues with the Crosswork Data Gateway VM.

Note

1. Some options may be restricted for the **dg-oper** user. See Table 1.
2. Crosswork Cloud does not support the **Remove All Non-Infra Containers and Reboot** option under the **Troubleshooting** menu.

The **Troubleshooting** menu provides the options listed here:

- Diagnostic commands, on page 499
- Run the Showtech command, on page 504
- Crosswork Data Gateway VMs reboots, on page 505
- Crosswork Data Gateway VMs shutdown, on page 505
- Export the auditd logs, on page 505
- Enable the TAC shell access, on page 506

Diagnostic commands

The **Run Diagnostics** menu provides you these options in the console:

Figure 113: Run diagnostics

Ping a host

The Crosswork Data Gateway provides a ping utility to check the reachability of any IP address.

Procedure

Step 1 From the **Main Menu**, select **Troubleshooting** > **Run Diagnostics** > **Ping**.

Step 2 Enter the required information:

- **Number of pings**: Specify how many pings to send.
- **Destination hostname or IP**: Enter the target hostname or IP address.
- **Source port**: Choose the type (UDP, TCP, or TCP Connect).
- **Destination port**: Select the appropriate type (UDP, TCP, or TCP Connect).

Step 3 Click **OK**.

Traceroute to a Host

The Crosswork Data Gateway offers the Traceroute option to help troubleshoot latency issues. This tool provides an estimate of the time it takes for the gateway to reach the destination.

Procedure

Step 1 From the **Main Menu**, select **Troubleshooting** > **Run Diagnostics** > **Traceroute**.

Step 2 Specify the destination for the traceroute.

Step 3 Click **OK**.

Troubleshoot the commands in Crosswork Data Gateway

The Crosswork Data Gateway provides a set of diagnostic commands to assist with troubleshooting.

Procedure

Step 1 From the Main Menu, navigate to **Troubleshooting** > **Run Diagnostics**.

Step 2 Choose one of the following commands based on your troubleshooting needs:

- **4 top**
- **5 lsof**
- **6 iostat**
- **7 vmstat**
- **8 nsolookup**

Apply any relevant filters or options for the selected command.

Step 3 Click **OK**.

Crosswork Data Gateway clears the screen and executes the selected command with the specified options.

Download the tcpdump

The tcpdump utility allows you to capture and analyze network traffic on Crosswork Data Gateway.

Note Only the **dg-admin** user can run the tcpdump utility.

Procedure

Step 1 From the Main Menu, navigate to **Troubleshooting** > **Run Diagnostics** > **tcpdump**.

Step 2 Choose an interface to run tcpdump on. To capture traffic from all interfaces, select the **All** option.

Step 3 Select whether to display packet information on screen or save it to a file.

Step 4 Set the following parameters:

- Packet count limit
- Collection time limit
- File size limit
- Filter expression

Step 5 Click **OK**.

- When tcpdump reaches the specified limits, Crosswork Data Gateway will:
  - Compress the capture file.
  - Prompt for **SCP credentials** to transfer the file to a remote host.
- Once the file transfer is complete (or canceled), the compressed file is deleted.

Run a controller session test

To verify if Crosswork Data Gateway can establish a connection to Crosswork Cloud, use the Controller Session Test. This test also checks whether the VM's resource allocation matches the deployment profile.

Procedure

From the **Main Menu**, navigate to **Troubleshooting** > **Run Diagnostics** > **Run Controller Session Test**.

If the connection is successful, a message confirming the connection appears. If the connection fails, the console displays these details to help you troubleshoot:

- DNS server IP address
- DNS domain
- NTP server address
- NTP status
- Proxy URL
- Proxy reachability status
- Controller URL
- Controller reachability status
- Last test date

Figure 114: Run Controller Session Tests menu

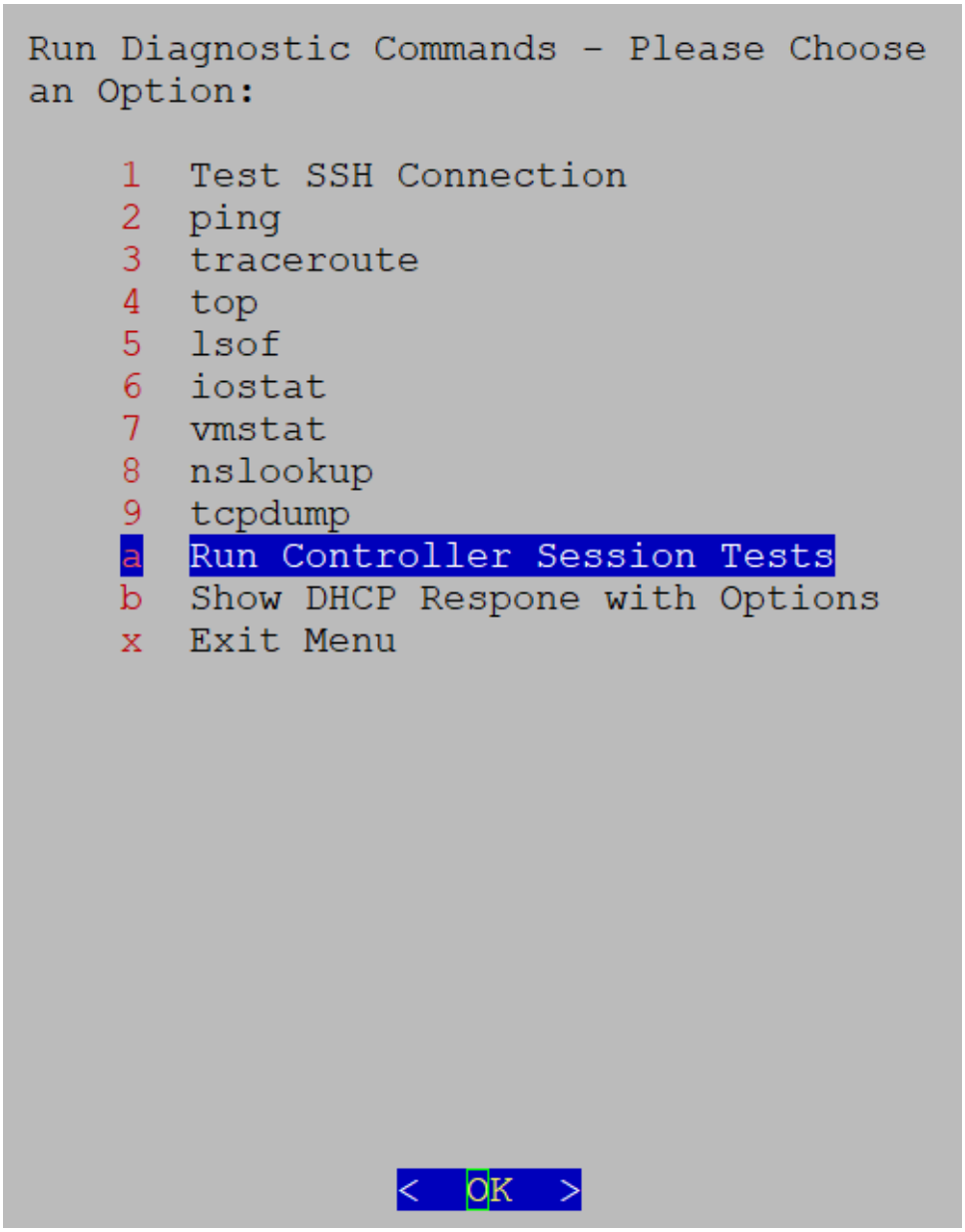
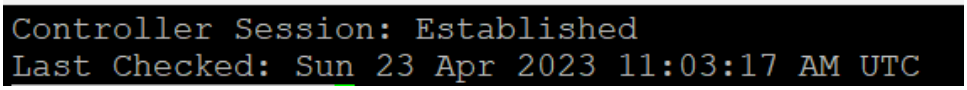


Figure 115: Result of the Run Controller Session Tests menu



What to do next

If the session test fails, review the displayed information to determine the probable cause. Follow the corrective actions suggested by the console.

Run the Showtech command

The Showtech command allows you to export logs and vital information from the Crosswork Data Gateway to a user-defined SCP destination.

Typically, the command enables you to collect:

- Logs from all Crosswork Data Gateway components running on Docker containers
- VM vitals

When you run the command, it creates a tarball in the directory where it is executed. The tarball is named `DG-<CDG version>-<CDG host name>-year-month-day--hour-minute-second.tar.xz.enc`.

Procedure

Step 1 From the **Troubleshooting** menu, select **Show-tech** and click **OK**.

Step 2 Specify where to save the tarball containing logs and VM vitals.

Step 3 Enter your **SCP passphrase** and click **OK**.

The **show-tech** file is downloaded in an encrypted format.

Note
The download may take several minutes depending on the system usage.

Step 4 After the download is complete, run the following command to decrypt it:

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

For 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.
- Do not enclose the filenames `<showtech file>` and `<decrypted filename>` in quotation marks.
- To decrypt on a MAC, you need OpenSSL 1.1.1+, as LibreSSL does not support all the necessary switches.

Crosswork Data Gateway VMs reboots

ou can reboot the VM in two ways using Crosswork Data Gateway.

- **Remove all Collectors and Reboot VM**: Select this option if you want to
  - stop containers that are downloaded after installation (collectors and offload containers).
  - remove Docker images associated with these containers.
  - remove collector data and configurations.
  - reboot the VM.

  This action restores the VM to its state immediately after the initial configuration, with only infrastructure containers running.
- **Reboot VM**: Select this option to perform a normal reboot of the Crosswork Data Gateway VM.

Note This task is only available to **dg-admin** users.

Crosswork Data Gateway VMs shutdown

From the Troubleshooting menu, select **5 Shutdown VM** to power off the Crosswork Data Gateway VM.

Export the auditd logs

Follow the steps to export auditd logs.

Procedure

Step 1 From **Troubleshooting**, select **Export Audit Logs**.

Step 2 Enter a passphrase to encrypt the auditd log tarball.

Step 3 Click **OK**.

Re-enroll Crosswork Data Gateway

To re-enroll Crosswork Data Gateway, complete each step in this task.

Before you begin

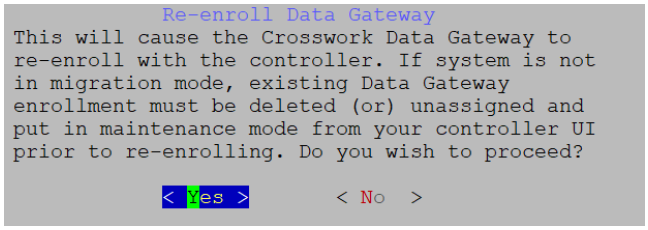
Before you re-enroll Crosswork Data Gateway, delete the existing enrollment from the controller.

Procedure

Step 1 From the **Troubleshooting** menu, select **Re-enroll Data Gateway**.

Step 2 Review the information in the confirmation window and click **Yes** to proceed.

Figure 116: Re-enroll Data Gateway Confirmation Window



Remove the rotated log files

To remove all rotated log files such as those with the .gz or .xz extension from the `/var/log` and `/opt/dg/log` folders, perform these steps:

Procedure

Step 1 From the **Troubleshooting** menu, select **Remove Rotated Log Files**.

Step 2 In the dialog that appears, select **Yes** to confirm and proceed with the log removal.

Enable the TAC shell access

The **TAC Shell Access** function allows a Cisco engineer to log in directly to the Ubuntu shell using multifactor authentication through the **dg-tac** user.

By default, the **dg-tac** account is locked and the password is expired to prevent unauthorized access. Once enabled, the **dg-tac** user is active for less than 24 hours (until midnight UTC [00:00 UTC] the next day).

Before you begin

Confirm that the Cisco engineer you are working with has access to the Secure Web Identity Management Service (SWIMS) Aberto tool. Active communication with the Cisco engineer is required to enable **dg-tac** access.

- Enabling this access requires you to communicate actively with the Cisco engineer.

Procedure

Step 1 Log in to the Crosswork Data Gateway VM as the **dg-admin** user.

Step 2 From the **Main Menu**, select **Troubleshooting**.

Step 3 From the **Troubleshooting** menu, select **Enable TAC Shell Access**.

A dialog appears, warning you that the **dg-tac** user login requires a password you set, along with a challenge token from TAC. Choose **Yes** to continue or **No** to cancel.

Step 4 If you proceed, the system prompts you to set a password for the **dg-tac** user.

Step 5 Enter a password, and the system displays the expiration date when the account will be disabled.

Step 6 Log out of Crosswork Data Gateway.

Step 7 If the Cisco engineer has direct access to the **Crosswork Data Gateway VM**, share the password you set in Step 3.

a) Share the password that you had set in Step 5 for the **dg-tac** user with the Cisco engineer who is working with you.
b) The engineer logs in via SSH as the **dg-tac** user with the password you provided.

The system will then prompt for a challenge token. The engineer signs it using SWIMS Aberto, pastes the signed response into the VM, and logs in successfully.

c) The Cisco engineer logs in successfully as the **dg-tac** user and completes the troubleshooting.

There is a fifteen-minute idle timeout period for the **dg-tac** user. If the Cisco engineer logs out, they must sign a new challenge to log in again.

d) After troubleshooting is complete, the Cisco engineer logs out of the TAC shell.

Step 8 If the Cisco engineer does not have direct access:

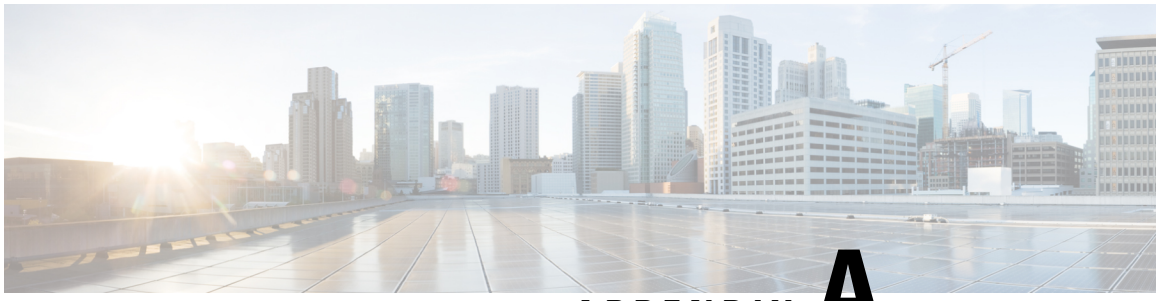
a) Start a meeting with desktop sharing enabled.
b) Log in as **dg-tac** using SSH:

```
ssh dg-tac@<DG hostname or IP>
```

c) Enter the password that you set and obtain the challenge token.
d) Share the token with the Cisco engineer, who will sign it using SWIMS Aberto and provide the signed response.
e) Paste the signed response back into the VM to get the shell prompt.
f) Share your desktop, or follow the engineer's instructions to troubleshoot.

There is a fifteen-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer must sign a new challenge to log in again.

g) Once troubleshooting is complete, the engineer logs out of the TAC shell.



APPENDIX A

List of Pre-loaded Traps and MIBs for SNMP Collection

This section contains the following topics:

List of pre-loaded traps and MIBs for SNMP collection

This section lists the traps and MIBs that the Cisco Crosswork Data Gateway supports for SNMP collection.

Note This list applies only when Crosswork Network Controller is the target application and is not limited if the target is an external application.

Important Contraints

- The system cannot extract index values from OIDs of conceptual tables. If any column that defines indices in a conceptual table is not populated, the system replaces the index value on the data plane with the instance identifier (OID suffix) of the row.
- The system cannot extract index values from conceptual tables that include the **AUGMENT** keyword or refer to indices of other tables.
- Named-number enumerations (using the integer syntax) are sent on the wire using their numeric value.

Table 90: Supported Traps

Trap	OID
linkDown	1.3.6.1.6.3.1.1.5.3
linkUp	1.3.6.1.6.3.1.1.5.4
coldStart	1.3.6.1.6.3.1.1.5.1
isisAdjacencyChange	1.3.6.1.2.1.138.0.17

List of Pre-loaded Traps and MIBs for SNMP Collection

Table 91: Supported MIBs

ADSL-LINE-MIB.mib	CISCO-LWAPP-INTERFACE-MIB.mib	IANA-ITU-ALARM-TC-MIB.mib
ADSL-TC-MIB.mib	CISCO-LWAPP- IPS-MIB.mib	IANA-LANGUAGE- MIB.mib
AGENTX-MIB.mib	CISCO-LWAPP-LINKTEST-MIB.mib	IANA-RTPROTO- MIB.mib
ALARM-MIB.mib	CISCO-LWAPP-LOCAL-AUTH-MIB.mib	IANAifType-MIB.mib
APS-MIB.mib	CISCO-LWAPP- MDNS-MIB.mib	IEEE8021-CFM-MIB.mib
ATM-FORUM-MIB.mib	CISCO-LWAPP-MESH-BATTERY-MIB.mib	IEEE8021-PAE-MIB.mib
ATM-FORUM- TC-MIB.mib	CISCO-LWAPP-MESH-LINKTEST-MIB.mib	IEEE8021-TC-MIB.mib
ATM-MIB.mib	CISCO-LWAPP-MOBILITY-EXT-MIB.mib	IEEE802171-CFM- MIB.mib
ATM-TC-MIB.mib	CISCO-LWAPP-MOBILITY-MIB.mib	IEEE8023-LAG-MIB.mib
ATM2-MIB.mib	CISCO-LWAPP-NETFLOW-MIB.mib	IEEE802dot11-MIB.mib
BGP4-MIB.mib	CISCO-LWAPP- REAP-MIB.mib	IF-INVERTED-STACK-MIB.mib
BRIDGE-MIB.mib	CISCO-LWAPP- RF-MIB.mib	IF-MIB.mib
CISCO-AAA- SERVER-MIB.mib	CISCO-LWAPP- SI-MIB.mib	IGMP-STD-MIB.mib
CISCO-AAA- SESSION-MIB.mib	CISCO-LWAPP- TC-MIB.mib	INET-ADDRESS-MIB.mib
CISCO-AAL5-MIB.mib	CISCO-LWAPP-TRUSTSEC-MIB.mib	INT-SERV-MIB.mib
CISCO-ACCESS-ENVMON-MIB.mib	CISCO-LWAPP- TSM-MIB.mib	INTEGRATED-SERVICES -MIB.mib
CISCO-ATM-EXT -MIB.mib	CISCO-LWAPP- WLAN-MIB.mib	IP-FORWARD-MIB.mib
CISCO-ATM-PVCTRAP-EXTN-MIB.mib	CISCO-LWAPP-WLAN -SECURITY-MIB.mib	IP-MIB.mib
CISCO-ATM- QOS-MIB.mib	CISCO-MEDIA-GATEWAY-MIB.mib	IPMCAST-MIB.mib
CISCO-AUTH-FRAMEWORK-MIB.mib	CISCO-MOTION-MIB.mib	IPMROUTE-MIB.mib

CISCO-BGP-POLICY -ACCOUNTING-MIB.mib	CISCO-MPLS-LSR -EXT-STD-MIB.mib	IPMROUTE-STD -MIB.mib
CISCO-BGP4-MIB.mib	CISCO-MPLS-TC -EXT-STD-MIB.mib	IPV6-FLOW-LABEL -MIB.mib
CISCO-BULK-FILE -MIB.mib	CISCO-MPLS-TE-STD -EXT-MIB.mib	IPV6-ICMP-MIB.mib
CISCO-CBP-TARGET -MIB.mib	CISCO-NAC-TC -MIB.mib	IPV6-MIB.mib
CISCO-CBP-TARGET -TC-MIB.mib	CISCO-NBAR-PROTOCOL -DISCOVERY-MIB.mib	IPV6-MLD-MIB.mib
CISCO-CBP-TC-MIB.mib	CISCO-NETSYNC -MIB.mib	IPV6-TC.mib
CISCO-CCME-MIB.mib	CISCO-NTP-MIB.mib	IPV6-TCP-MIB.mib
CISCO-CDP-MIB.mib	CISCO-OSPF- MIB.mib	IPV6-UDP-MIB.mib
CISCO-CEF-MIB.mib	CISCO-OSPF- TRAP-MIB.mib	ISDN-MIB.mib
CISCO-CEF-TC.mib	CISCO-OTN-IF-MIB.mib	ISIS-MIB.mib
CISCO-CLASS-BASED -QOS-MIB.mib	CISCO-PAE-MIB.mib	ITU-ALARM-MIB.mib
CISCO-CONFIG- COPY-MIB.mib	CISCO-PAGP-MIB.mib	ITU-ALARM-TC- MIB.mib
CISCO-CONFIG- MAN-MIB.mib	CISCO-PIM-MIB.mib	L2TP-MIB.mib
CISCO-CONTENT-ENGINE-MIB.mib	CISCO-PING-MIB.mib	LANGTAG-TC-MIB.mib
CISCO-CONTEXT-MAPPING-MIB.mib	CISCO-POLICY-GROUP -MIB.mib	LLDP-EXT-DOT1 -MIB.mib
CISCO-DATA -COLLECTION-MIB.mib	CISCO-POWER-ETHERNET-EXT-MIB.mib	LLDP-EXT-DOT3 -MIB.mib
CISCO-DEVICE-EXCEPTION -REPORTING-MIB.mib	CISCO-PRIVATE -VLAN-MIB.mib	LLDP-MIB.mib
CISCO-DIAL- CONTROL-MIB.mib	CISCO-PROCESS-MIB.mib	MAU-MIB.mib
CISCO-DOT11-ASSOCIATION-MIB.mib	CISCO-PRODUCTS- MIB.mib	MGMD-STD-MIB.mib
CISCO-DOT11-HT- PHY-MIB.mib	CISCO-PTP-MIB.mib	MPLS-FTN-STD- MIB.mib
CISCO-DOT11-IF-MIB.mib	CISCO-RADIUS- EXT-MIB.mib	MPLS-L3VPN-STD- MIB.mib
CISCO-DOT11-SSID-SECURITY-MIB.mib	CISCO-RF-MIB.mib	MPLS-LDP-ATM-STD-MIB.mib

List of Pre-loaded Traps and MIBs for SNMP Collection

CISCO-DOT3- OAM-MIB.mib	CISCO-RF-SUPPLEMENTAL -MIB.mib	MPLS-LDP-FRAME -RELAY-STD-MIB.mib
CISCO-DS3-MIB.mib	CISCO-RTTMON-TC -MIB.mib	MPLS-LDP-GENERIC-STD-MIB.mib
CISCO-DYNAMIC-TEMPLATE-MIB.mib	CISCO-SELECTIVE-VRF-DOWNLOAD-MIB.mib	MPLS-LDP-MIB.mib
CISCO-DYNAMIC -TEMPLATE-TC-MIB.mib	CISCO-SESS-BORDER-CTRLR -CALL-STATS-MIB.mib	MPLS-LDP-STD-MIB.mib
CISCO-EIGRP-MIB.mib	CISCO-SESS-BORDER-CTRLR-EVENT-MIB.mib	MPLS-LSR-MIB.mib
CISCO-EMBEDDED-EVENT-MGR-MIB.mib	CISCO-SESS-BORDER-CTRLR-STATS-MIB.mib	MPLS-LSR-STD-MIB.mib
CISCO-ENHANCED-IMAGE-MIB.mib	CISCO-SMI.mib	MPLS-TC-MIB.mib
CISCO-ENHANCED-MEMPOOL-MIB.mib	CISCO-SONET-MIB.mib	MPLS-TC-STD-MIB.mib
CISCO-ENTITY-ASSET -MIB.mib	CISCO-ST-TC.mib	MPLS-TE-MIB.mib
CISCO-ENTITY-EXT -MIB.mib	CISCO-STACKWISE- MIB.mib	MPLS-TE-STD-MIB.mib
CISCO-ENTITY-FRU-CONTROL-MIB.mib	CISCO-STP-EXTENSIONS -MIB.mib	MPLS-VPN-MIB.mib
CISCO-ENTITY- QFP-MIB.mib	CISCO-SUBSCRIBER -IDENTITY-TC-MIB.mib	MSDP-MIB.mib
CISCO-ENTITY-REDUNDANCY-MIB.mib	CISCO-SUBSCRIBER-SESSION-MIB.mib	NET-SNMP-AGENT -MIB.mib
CISCO-ENTITY-REDUNDANCY-TC-MIB.mib	CISCO-SUBSCRIBER-SESSION-TC-MIB.mib	NET-SNMP-EXAMPLES -MIB.mib
CISCO-ENTITY- SENSOR-MIB.mib	CISCO-SYSLOG-MIB.mib	NET-SNMP-MIB.mib
CISCO-ENTITY-VENDORTYPE-OID-MIB.mib	CISCO-SYSTEM-EXT- MIB.mib	NET-SNMP-TC.mib
CISCO-ENVMON-MIB.mib	CISCO-SYSTEM-MIB.mib	NHRP-MIB.mib
CISCO-EPM-NOTIFICATION-MIB.mib	CISCO-TAP2-MIB.mib	NOTIFICATION-LOG-MIB.mib
CISCO-ETHER-CFM- MIB.mib	CISCO-TC.mib	OLD-CISCO-CHASSIS-MIB.mib
CISCO-ETHERLIKE- EXT-MIB.mib	CISCO-TCP-MIB.mib	OLD-CISCO-INTERFACES -MIB.mib

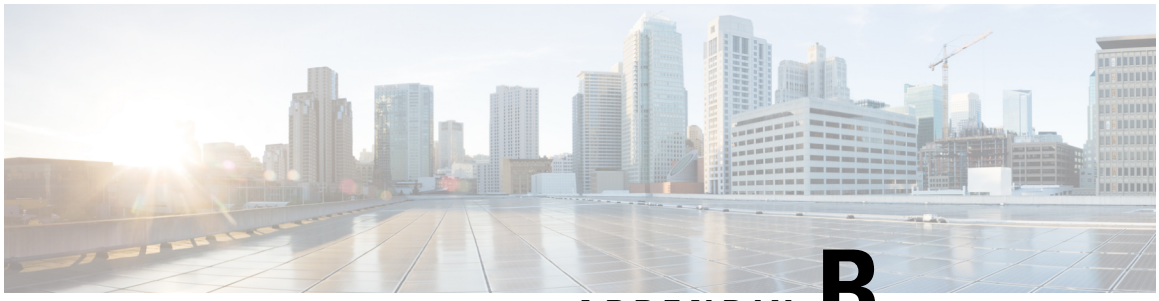
CISCO-FABRIC- C12K-MIB.mib	CISCO-TEMP-LWAPP -DHCP-MIB.mib	OLD-CISCO-SYS- MIB.mib
CISCO-FIREWALL -TC.mib	CISCO-TRUSTSEC -SXP-MIB.mib	OLD-CISCO-SYSTEM -MIB.mib
CISCO-FLASH-MIB.mib	CISCO-TRUSTSEC -TC-MIB.mib	OPT-IF-MIB.mib
CISCO-FRAME- RELAY-MIB.mib	CISCO-UBE-MIB.mib	OSPF-MIB.mib
CISCO-FTP-CLIENT -MIB.mib	CISCO-UNIFIED-COMPUTING-ADAPTOR -MIB.mib	OSPF-TRAP-MIB.mib
CISCO-HSRP-EXT -MIB.mib	CISCO-UNIFIED-COMPUTING-COMPUTE -MIB.mib	OSPFV3-MIB.mib
CISCO-HSRP-MIB.mib	CISCO-UNIFIED-COMPUTING-ETHER -MIB.mib	P-BRIDGE-MIB.mib
CISCO-IETF-ATM2 -PVCTRAP-MIB.mib	CISCO-UNIFIED-COMPUTING-FC- MIB.mib	PIM-MIB.mib
CISCO-IETF-BFD -MIB.mib	CISCO-UNIFIED-COMPUTING-MEMORY -MIB.mib	PIM-STD-MIB.mib
CISCO-IETF-FRR -MIB.mib	CISCO-UNIFIED- COMPUTING -MIB.mib	POWER-ETHERNET -MIB.mib
CISCO-IETF-IPMROUTE -MIB.mib	CISCO-UNIFIED-COMPUTING-NETWORK -MIB.mib	PPP-IP-NCP-MIB.mib
CISCO-IETF-ISIS -MIB.mib	CISCO-UNIFIED-COMPUTING-PROCESSOR -MIB.mib	PPP-LCP-MIB.mib
CISCO-IETF-MPLS-ID -STD-03-MIB.mib	CISCO-UNIFIED-COMPUTING-TC- MIB.mib	PPVPN-TC-MIB.mib
CISCO-IETF-MPLS-TE-EXT-STD-03- MIB.mib	CISCO-VLAN-IFTABLE-RELATIONSHIP -MIB.mib	PTOPO-MIB.mib
CISCO-IETF-MPLS-TE-P2MP-STD-MIB.mib	CISCO-VLAN-MEMBERSHIP-MIB.mib	PerfHist-TC-MIB.mib
CISCO-IETF-MSDP -MIB.mib	CISCO-VOICE-COMMON -DIAL-CONTROL-MIB.mib	Q-BRIDGE-MIB.mib
CISCO-IETF-PIM-EXT -MIB.mib	CISCO-VOICE-DIAL -CONTROL-MIB.mib	RADIUS-ACC-CLIENT -MIB.mib
CISCO-IETF-PIM -MIB.mib	CISCO-VOICE-DNIS -MIB.mib	RADIUS-AUTH-CLIENT -MIB.mib

List of Pre-loaded Traps and MIBs for SNMP Collection

CISCO-IETF-PW- ATM-MIB.mib	CISCO-VPDN-MGMT -MIB.mib	RFC-1212.mib
CISCO-IETF-PW- ENET-MIB.mib	CISCO-VTP-MIB.mib	RFC-1215.mib
CISCO-IETF-PW-MIB.mib	CISCO-WIRELESS-NOTIFICATION-MIB.mib	RFC1155-SMI.mib
CISCO-IETF-PW- MPLS-MIB.mib	CISCOSB-DEVICEPARAMS -MIB.mib	RFC1213-MIB.mib
CISCO-IETF-PW -TC-MIB.mib	CISCOSB- HWENVIROMENT.mib	RFC1315-MIB.mib
CISCO-IETF-PW -TDM-MIB.mib	CISCOSB-MIB.mib	RFC1398-MIB.mib
CISCO-IETF-VPLS -BGP-EXT-MIB.mib	CISCOSB-Physicaldescription -MIB.mib	RIPv2-MIB.mib
CISCO-IETF-VPLS -GENERIC-MIB.mib	DIAL-CONTROL-MIB.mib	RMON-MIB.mib
CISCO-IETF-VPLS- LDP-MIB.mib	DIFFSERV-DSCP-TC.mib	RMON2-MIB.mib
CISCO-IF-EXTENSION -MIB.mib	DIFFSERV-MIB.mib	RSTP-MIB.mib
CISCO-IGMP-FILTER -MIB.mib	DISMAN-NSLOOKUP -MIB.mib	RSVP-MIB.mib
CISCO-IMAGE-LICENSE -MGMT-MIB.mib	DISMAN-PING-MIB.mib	SMON-MIB.mib
CISCO-IMAGE-MIB.mib	DISMAN-SCHEDULE -MIB.mib	SNA-SDLC-MIB.mib
CISCO-IMAGE-TC.mib	DISMAN-SCRIPT-MIB.mib	SNMP-COMMUNITY -MIB.mib
CISCO-IP-LOCAL- POOL-MIB.mib	DISMAN-TRACEROUTE -MIB.mib	SNMP-FRAMEWORK -MIB.mib
CISCO-IP-TAP-MIB.mib	DOT3-OAM-MIB.mib	SNMP-MPD-MIB.mib
CISCO-IP-URPF-MIB.mib	DRAFT-MSDP-MIB.mib	SNMP-NOTIFICATION -MIB.mib
CISCO-IPMROUTE- MIB.mib	DS0-MIB.mib	SNMP-PROXY-MIB.mib
CISCO-IPSEC-FLOW -MONITOR-MIB.mib	DS1-MIB.mib	SNMP-REPEATER -MIB.mib
CISCO-IPSEC-MIB.mib	DS3-MIB.mib	SNMP-TARGET-MIB.mib
CISCO-IPSEC-POLICY -MAP-MIB.mib	ENTITY-MIB.mib	SNMP-USER-BASED -SM-MIB.mib
CISCO-IPSLA-AUTOMEASURE-MIB.mib	ENTITY-SENSOR-MIB.mib	SNMP-USM-AES -MIB.mib

CISCO-IPSLA- ECHO-MIB.mib	ENTITY-STATE-MIB.mib	SNMP-USM-DH-OBJECTS-MIB.mib
CISCO-IPSLA- JITTER-MIB.mib	ENTITY-STATE- TC-MIB.mib	SNMP-VIEW-BASED-ACM-MIB.mib
CISCO-IPSLA- TC-MIB.mib	ESO-CONSORTIUM -MIB.mib	SNMPv2-CONF.mib
CISCO-ISDN-MIB.mib	ETHER-WIS.mib	SNMPv2-MIB.mib
CISCO-LICENSE- MGMT-MIB.mib	EtherLike-MIB.mib	SNMPv2-SMI.mib
CISCO-LOCAL-AUTH-USER-MIB.mib	FDDI-SMT73-MIB.mib	SNMPv2-TC-v1.mib
CISCO-LWAPP- AAA-MIB.mib	FR-MFR-MIB.mib	SNMPv2-TC.mib
CISCO-LWAPP- AP-MIB.mib	FRAME-RELAY -DTE-MIB.mib	SNMPv2-TM.mib
CISCO-LWAPP- CCX-RM-MIB.mib	FRNETSERV- MIB.mib	SONET-MIB.mib
CISCO-LWAPP- CDP-MIB.mib	GMPLS-LSR- STD-MIB.mib	SYSAPPL-MIB.mib
CISCO-LWAPP-CLIENT -ROAMING-CAPABILITY.mib	GMPLS-TC-STD- MIB.mib	TCP-MIB.mib
CISCO-LWAPP-CLIENT -ROAMING-MIB.mib	GMPLS-TE-STD-MIB.mib	TOKEN-RING-RMON -MIB.mib
CISCO-LWAPP-DHCP -MIB.mib	HC-PerfHist-TC-MIB.mib	TOKENRING-MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CALIB-MIB.mib	HC-RMON-MIB.mib	TRANSPORT-ADDRESS -MIB.mib
CISCO-LWAPP-DOT11-CLIENT-CCX-TC-MIB.mib	HCNUM-TC.mib	TUNNEL-MIB.mib
CISCO-LWAPP-DOT11 -LDAP-MIB.mib	HOST-RESOURCES -MIB.mib	UDP-MIB.mib
CISCO-LWAPP- DOT11-MIB.mib	HOST-RESOURCES -TYPES.mib	VPN-TC-STD-MIB.mib
CISCO-LWAPP -DOWNLOAD-MIB.mib	IANA-ADDRESS-FAMILY-NUMBERS-MIB.mib	VRRP-MIB.mib
CISCO-LWAPP- IDS-MIB.mib	IANA-GMPLS-TC-MIB.mib	

List of Pre-loaded Traps and MIBs for SNMP Collection



APPENDIX B

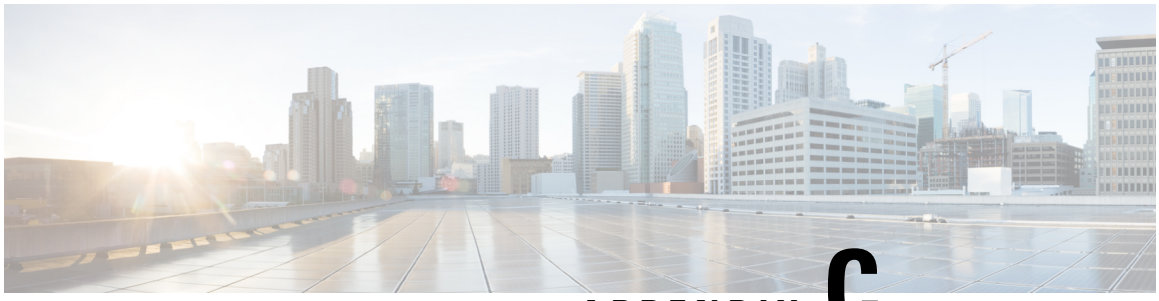
List of Pre-loaded YANG Modules for MDT Collection

This section contains the following topics:

List of pre-loaded YANG modules for MDT collection

This section lists the YANG modules that Crosswork Data Gateway supports for MDT collection on Cisco IOS XR devices.

List of Pre-loaded YANG Modules for MDT Collection



APPENDIX C

Cisco EPM Notification MIB

This section contains the following topics:

Cisco EPM Notification MIB

This table provides the mapping of event fields to the alarm model in CISCO-EPM-NOTIFICATION-MIB.

Note Some of the values in this table may appear truncated in a PDF. Refer to the HTML version of this content for a clearer view of the values.

Table 92: Cisco-EPM-Notification-MIB

Event Field	Snmpvarbind	OID	Description
TimeStamp	cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	The time when the event was raised. Example: 1639759929
AlarmId	cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	The unique alarm instance ID. Example: 57e3ef70-1597
Type	cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	Type of event Example : 2001
Category	cenAlarmCategory	1.3.6.1.4.9.9.311.1.1.2.1.9	The category of the event generated represented in an integer value. *System = 3, Network = 7, Audit = 13; Security = 4, External = 1* Example: 3

Event Field	Snmpvarbind	OID	Description
Category Definition	cenAlarmCategoryDefinition	1.3.6.1.4.9.9.311.1.1.2.1.10	The short description of the category of the event. The format is '<integer, eventCategory description>. Example: 3, System
Address Type	cenAlarmServerAddressType	1.3.6.1.4.9.9.311.1.1.2.1.11	The type of internet address of the CW alarm centre (VIP). Example: 1:ipv4, 2:ipv6
Address	cenAlarmServerAddress	1.3.6.1.4.9.9.311.1.1.2.1.12	The IP Address of the CW alarm centre (VIP). Example: 10.127.101.145
OriginAppId	cenAlarmManagedObjectClass	1.3.6.1.4.1.9.9.311.1.1.2.1.13	This attribute contains the OriginAppId of the application which generated the event. Example: DLM
Description	cenAlarmDescription	1.3.6.1.4.9.9.311.1.1.2.1.16	A detailed description of the event. Example:Reachability request did not receive any response from CDG
Severity	cenAlarmSeverity	1.3.6.1.4.9.9.311.1.1.2.1.17	The alarm severity indicates the severity of the event in an integer value. Critical=2; Major=3; Warning=4; Minor=5, Info=6, Clear=7 Example: 5
Severity definition	cenAlarmSeverityDefinition	1.3.6.1.4.9.9.311.1.1.2.1.18	The short description of the severity of the event. The string uses the format '<integer, eventSeverity description>'. Example: 3,Major
ObjectDescription, ObjectId	cenUserMessage1	1.3.6.1.4.1.9.9.311.1.1.2.1.21	Information about the event ObjectDescription, ObjectId. The string uses the format '<ObjectDescription=xx, ObjectId=xx>'. Example: ObjectDescription= Node<xrvr9k>, ObjectId= NodeData [4a16368]
OriginServiceId	cenUserMessage2	1.3.6.1.4.1.9.9.311.1.1.2.1.22	Information about the event OriginServiceId. Example: 0

Event Field	Snmpvarbind	OID	Description
EventId	cenAlertID	1.3.6.1.4.9.9.311.1.1.2.1.29	This attribute will contain the event ID of the generated event. Example: 9f19e5a9-a64c
cenAlarmVersion	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.2	The release version of this MIB. Example: 1.0
Timestamp	cenAlarmTimestamp	1.3.6.1.4.9.9.311.1.1.2.1.3	The time when the alarm or event was raised. Note: This is the number of seconds since January 1st 1970 (since epoch) in UTC Example:1523608787
Timestamp	cenAlarmUpdatedTimestamp	1.3.6.1.4.9.9.311.1.1.2.1.4	Alarms or events persist over time, and the value updates automatically when field(s) change. The updated time denotes a time. Each alarm is identified by the unique alarm instance ID. For example, cenAlarmInstanceID
cenAlarmInstanceID	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.5	The Unique Alarm Instance ID. Example: c2afd3c1-d4e5-46db-84b2- 86d0d43f2056
cenAlarmStatus	Integer	1.3.6.1.4.9.9.311.1.1.2.1.6	The alarm status indicates the status of the alarm in integer value. Example: Active=2, Cleared=3
cenAlarmStatus Definition	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.7	The short description of the status of the alarm. The string consists of comma-separated tuples. The value is the same value that the 'cenAlarmStatus'attribute holds. Contains one line description of the alarm status generated. Example: 2, ACTIVE 3, CLEARED

Event Field	Snmpvarbind	OID	Description
cenAlarmType	Integer	1.3.6.1.4.9.9.311.1.1.2.1.8	• unknown(1) —When the value for this attribute could not be determined. • direct(2)— Denotes an alarm generated by a set of events where all events are reported by an observation(s) of a managed object. • indirect(3)—Denotes an alarm generated by a set of events where all events were deduced or inferred by the status of managed objects as determined by the network management system. • mixed(4)—Denotes an alarm generated by a set of events which were either direct or indirect. Example: 2
cenAlarmCategory	Integer	1.3.6.1.4.9.9.311.1.1.2.1.9	The category of the alarm or event generated represented in integer value. Note: This integer field is not used in Crosswork Network Controller. Use cenAlarmCategoryDefinition instead, which is a string.
cenAlarmCategory Definition	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.10	The short description of the alarm or event's category. The string consists of comma-separated tuples. The value is the same value that the 'cenAlarmCategory' attribute holds. Contains one line description of the alarm category generated. For a list of alarm types, refer Alarms and Events. Example: "LINK_DOWN", "SWT_AUTH_FAIL", "LINK_UP"

Event Field	Snmpvarbind	OID	Description
cenAlarmServer AddressType	InetAddressType	1.3.6.1.4.9.9.311.1.1.2.1.11	The type of Internet address by which the server is reachable. The server is the server that is generating this trap. Example: 0: unknown 1: ipv4 2: ipv6
cenAlarmServerAddress	InetAddress	1.3.6.1.4.9.9.311.1.1.2.1.12	The IP Address or the DNS name of the Management. Server that raised this alarm will be notified. Example: 10.127.101.145
cenAlarmManaged ObjectClass	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.13	The class of the managed object for which this alarm or event was generated such as router or switch. For a list of alarm types, refer Alarms and Events. Example: "Optical", "Carrier Ethernet"
cenAlarmManagedObject AddressType	InetAddressType	1.3.6.1.4.9.9.311.1.1.2.1.14	The type of Internet address by which the managed object is reachable. Example: 0: unknown 1: ipv4 2: ipv6
cenAlarmManaged ObjectAddress	InetAddress	1.3.6.1.4.9.9.311.1.1.2.1.15	The IP Address or the DNS name of the Managed Object. Example: 2405:200:204:138: 172:30:9:121
cenAlarmDescription	OctetString	1.3.6.1.4.9.9.311.1.1.2.1.16	A detailed description of the alarm or event. Example: Port 'GigabitEthernet0/0/6' (Description: '# TO GigabitEthernet0/0/7 #') is down on device '2405:200:204:138: 172:30:9:121'. :Lost Carrier

Event Field	Snmpvarbind	OID	Description
cenAlarmSeverity	Integer	1.3.6.1.4.9.9.311.1.1.2.1.17	The alarm severity indicates the severity of the alarm in integer value. • 1—Critical • 2—Major • 3—Minor • 4—Warning • 5—Clear • 6—Info
cenAlarmSeverity Definition	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.18	The short description of the severity of the alarm generated. The string consists of comma-separated tuples. The value is the same value that the 'cenAlarmSeverity ' attribute holds. Contains one line description of the alarm severity generated. • 1—Critical • 2—Major • 3—Minor • 4—Warning • 5—Clear • 6—Info
cenAlarmTriageValue	Integer	1.3.6.1.4.9.9.311.1.1.2.1.19	The triage value of an alarm is a hierarchical weighting value (applied by the application, and more importantly customizable by the end user) to allow an artificial form of evaluating impact, interest, or other user-determined functions between alarms. The value is a positive number or zero, which denotes an undetermined or uncomputable value. Note: Crosswork Network Controller does not support this field.
cenEventIDList	OctetString	1.3.6.1.4.9.9.311.1.1.2.1.20	Comma separated list of the unique event identifiers that led to the generation of this Alarm. Note: Crosswork Network Controller does not support this field.

Event Field	Snmpvarbind	OID	Description
cenUserMessage1	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.21	User input message. Information about the alarm including whether the alarm/event is a root cause alarm or a service - impacting alarm. srcObjectDisplayName= GigabitEthernet0/0/0/18, rootCauseId=0, hostName=ASR9001 156.156.cisco, serviceImpacting=0, applicationSpecificAlarmID= LINK_DOWN:10.127.101.156: If: GigabitEthernet0/0/0/18##SubAlarm@@_7, correlationType=UNKNOWN, srcObjectBusinessKey= 4c2b8aa7 [1589721133_10.127.101.156, GigabitEthernet0/0/0/18 chassisId = 0. srcObjectDisplayName refers to the Location in UI. chassisId refers to Satellite Id. If any of the above information is not populated, then corresponding value is not sent to NBI.
cenUserMessage2	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.22	User input message. This value can be configured. Note: Crosswork Network Controller does not support this field.
cenUserMessage3	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.23	User input message. This value can be configured. Note: Crosswork Network Controller does not support this field.

Event Field	Snmpvarbind	OID	Description
cenAlarmMode	Integer	1.3.6.1.4.9.9.311.1.1.2.1.24	• unknown(1) —When the value for this attribute could not be determined • alert(2) — Denotes an alarm generated by a set of events where all events are reported by polling of managed objects and/or listening to SNMP notifications • event(3) — Denotes an event generated by polling of managed objects and/or listening to SNMP notifications Example: 2
cenPartitionNumber	Integer	1.3.6.1.4.9.9.311.1.1.2.1.24	In traps generated by the management application that support multiple partitions, the attribute will carry the integer value assigned to identify the logical group where the managed device resides. Note: Crosswork Network Controller does not support this field.
cenPartitionName	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.26	In traps generated by the management application that support multiple partitions, the attribute will carry the name assigned to identify the logical group where the managed device resides.
cenCustomer Identification	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.27	User input message. The attribute takes in a free format text. This attribute can be used by advanced management applications to sort responses from the fault management server. Note: Crosswork Network Controller does not support this field.
cenCustomerRevision	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.28	User input message. The attribute takes in a free format text. This attribute can be used by advanced management applications to sort responses from the fault management server. Note: Crosswork Network Controller does not support this field.

Event Field	Snmpvarbind	OID	Description
cenAlertID	SnmpAdminString	1.3.6.1.4.9.9.311.1.1.2.1.29	In event based notification, this attribute will contain the alert ID to which the generated event has been rolled upto. In alert based notification, the cenAlarmInstanceId and cenAlertID will be identical. Example:1185098114

Cisco EPM Notification MIB