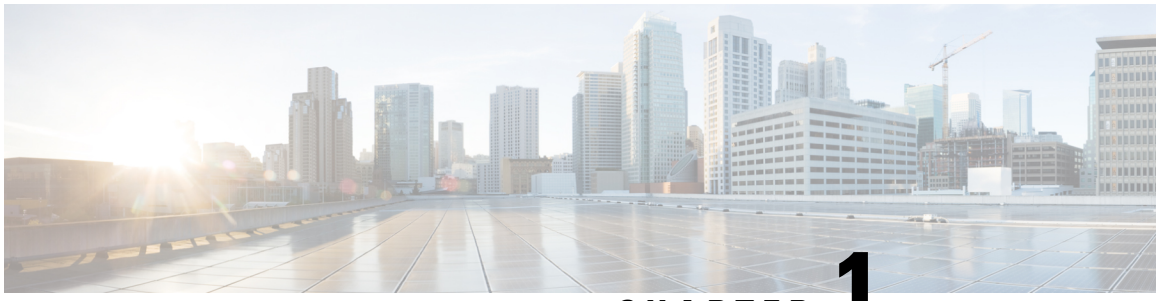
Cisco Crosswork Network Controller 7.0 Administration Guide

First Published: 2024-08-28

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

Get Up and Running (Post-Installation)

This section contains the following topics:

Before You Begin

Before using the Cisco Crosswork Network Controller applications, it is recommended that you familiarize yourself with basic concepts and complete necessary planning and information-gathering steps.:

- **User Roles**: Cisco recommends using role-based access control to restrict users to only the software functions necessary for their job duties. By default, new users have full administrative privileges. To avoid extending these privileges to every user, you should plan a system of user roles, create these roles, and assign them to user profiles accordingly.
- **User Accounts**: Cisco recommends creating separate accounts for all users to maintain an audit record of user activity on the system. Prepare a list of users for the Crosswork Network Controller applications, decide on their usernames and preliminary passwords, and create user profiles for them. Crosswork Network Controller also supports integration with TACACS+ and LDAP servers for centralized management of user roles and accounts. For more details, see Set Up User Authentication (TACACS+, LDAP, and RADIUS), on page 343.
- **Device-Access Groups**: Device-Access Groups (DAGs) are groups of devices that define device access for users. Users who are associated with DAGs can make configuration changes and provision services on the devices within those groups. When creating a user, you must assign them at least one DAG and a role. For more details, see Manage Device Access Groups, on page 332.
- **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. This includes user IDs, passwords, and additional data such as SNMPv2 read and write community strings, and SNMPv3 authentication and privilege types. For other providers

(NSO, SR-PCE, Storage, Alert, and WAE), this always includes 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, so you can use them to group your devices when you first onboard them. You don't need a complete list of tags initially, as you can always add more later. However, ensure that all the tags you plan to use are in place before you need them. Otherwise, you must manually go back and add them where you wish to use them. For more details, see Create Tags, on page 270.

- **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, a provider (for example, NSO, SR-PCE) must be configured for each external service. The provider family determines the type of service supplied to Crosswork Network Controller and the unique parameters that must be configured. 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 About Provider Families, on page 240 and Provider Dependency, on page 240.

  - 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 Add Cisco NSO Providers, on page 244.

Note Additional steps are required when using NSO in LSA mode. For more details on these steps, see Enable Layered Service Architecture (LSA), on page 247.

  - 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 either manually add devices to the system (see Add Devices to the Inventory, on page 275 for more details) or auto-onboard them via SR-PCE discovery (see Add Cisco SR-PCE Providers, on page 249 for more details). While you can change the configuration at any time, it is ideal to decide which process you will use before getting too far into the deployment and configuration of Crosswork Network Controller.

- **Devices**: You can onboard devices using the UI, a CSV file, an API, SR-PCE discovery, or zero touch provisioning. The method used to onboard a device determines the type of information needed to configure it 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 Add Devices to the Inventory, on page 275.

Note For information on device configuration, device monitoring, and device management workflows, see the *Crosswork Network Controller 7.0 Device Lifecycle Management* guide.

- **External Data Destination(s)**: 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. This is covered in detail in Cisco Crosswork Data Gateway, on page 45.
- **Labels**: Labels are used with Crosswork Change Automation 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.
- If you plan to use Crosswork Health Insights, **KPI (Key Performance Indicators) Profiles** are used to monitor the health of the network. 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.
- 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.

Setup Workflow

The first step in getting started with Crosswork Network Controller is to prepare the system for use. The table below provides topics to refer to for help when executing each of the following tasks:

Note This workflow assumes that you have already installed Crosswork Network Controller Applications and Crosswork Data Gateway. For the installation instructions, please refer to the latest version of *Cisco Crosswork Network Controller 7.0 Installation Guide*.

If you were able to complete the recommended planning steps explained in "Before you begin", you should have all the information you need to finish each step in this workflow.

Table 1: 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: Configuration Prerequisites for New Devices, on page 276 Sample Configuration for Cisco NSO Devices, on page 281
2. Create user accounts and user roles.	Follow the steps in Manage Users, on page 312 and Create User Roles, on page 315.
3. Create credential profiles.	Follow the steps in Create Credential Profiles, on page 232

Step	Action
4. Add the provider(s).	Follow the steps in About Adding Providers, on page 241
5. Validate communications with the provider(s).	Check on the provider's reachability using the steps in Get Provider Details, on page 266
6. Import or create tags.	To import them: Import Tags, on page 271 To create them: Create Tags, on page 270
7. Onboard your devices.	See Add Devices to the Inventory, on page 275. For more information, see the *Cisco Crosswork Network Controller 7.0 Device Lifecycle Management* guide.
8. Setup Crosswork Data Gateway	Follow the steps in Set Up Crosswork Data Gateway To Collect Data, on page 52.
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 7.0 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 Configure AAA Settings, on page 355.
11. (Optional) Create additional user accounts and user roles.	Follow the steps in Manage Users, on page 312 and Create User Roles, on page 315.
12. (Optional) Import or create additional credential profiles and providers.	To import providers: Import Providers, on page 265 To create providers: Add Providers Through the UI, on page 242
13. (Optional) Group your devices logically as per your requirement.	Follow the steps in Use Device Groups to Filter your Topology Map, on page 205.
14. (Optional) Set display preferences for your topology.	Follow the steps in Use Internal Maps Offline for Geographical Map Display, on page 204 and Show Link Health by Color, on page 223.

Log In and Log Out

The Crosswork Network Controller user interface is browser-based. For the supported browser versions, see the *Compatibility Information* section in the *Cisco Crosswork Network Controller 7.0 Release Notes*. .

Attention

- Crosswork Network Controller locks out users for a specified period of time after repeated unsuccessful login attempts. Users can attempt to log in with the correct credentials once the wait time is over. Users remain locked out until they enter the valid login credentials. The number of unsuccessful login attempts and the lockout time are configured by the administrators in the **Local Password Policy**. For more information, see Configure AAA Settings, on page 355.
- The Crosswork Network Controller login page is not rendered when the CAS (Central Authentication Service) pod is restarting or not running.
- If a user has multiple sessions open from same client (via multiple tabs/windows) and logout/terminate session is performed for that session from one of the windows, the logout screen is displayed on that window while the following error message is displayed on all other tabs/windows: `"Your session has ended. Log into the system again to continue"`.

Step 1 Open a web browser and enter:

`https://<Crosswork Management Network Virtual IP (IPv4)>:30603/`

or

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

Note

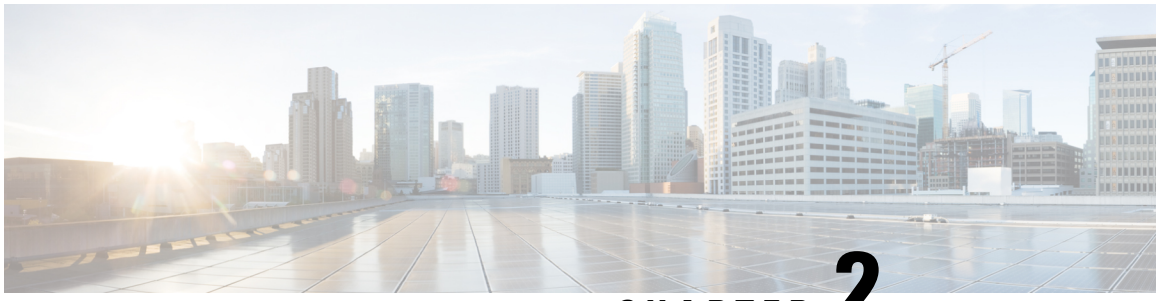
- The IPv6 address in the URL must be enclosed with brackets.
- When you access Crosswork Network Controller from your browser for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the server. After you do this, the browser accepts the Crosswork Network Controller server as a trusted site in all subsequent logins.

Step 2 The browser-based user interface displays the login window. Enter your username and password.

The default administrator user name and password is **admin**. This account is created automatically at installation (see Administrative Users Created During Installation, on page 314). The initial password for this account must be changed during installation verification. Cisco strongly recommends that you keep the default administrator credential secure, and never use it for routine logins. Instead, create new user roles with appropriate privileges and assign new users to those roles. At least one of the users you create must be assigned the "admin" role.

Step 3 Click **Log In**.

Step 4 To log out, click in the top right of the main window and choose **Log out**.



CHAPTER 2

Manage Backups

This section contains the following topics:

Backup and Restore Overview

Crosswork Network Controller's backup and restore features help prevent data loss and preserve your installed applications and settings.

Among the backup options, you can also choose to **Backup NSO**. This option preserves the Cisco NSO data along with the Crosswork Network Controller configuration. See Backup Crosswork Network Controller with NSO, on page 16 for details.

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

From the main menu, click **Administration** > **Backup and Restore** to access the **Backup and Restore** window.

Table 2: Backup and Restore options

Menu option	Description
Actions > Data Backup (See Manage Crosswork Network Controller Backup and Restore, on page 8 for details)	Preserves the Crosswork Network Controller configuration data. The backup file can be used with the data disaster restore (Restore Crosswork Network Controller After a Disaster, on page 11) to recover from a serious outage.

Menu option	Description
Actions > Data Disaster Restore (See Restore Crosswork Network Controller After a Disaster, on page 11 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 7.0 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.

Table 3: Supported Backup Restore Combinations

Backup Type	From Deployment	To Deployment	Support
Data only	Geo redundant	Geo redundant	Supported
Data only	Non-geo redundant	Non-geo redundant	Supported

Any other combination is not supported.

Manage Crosswork Network Controller Backup and Restore

This section explains how to perform a data backup and restore operation from the Crosswork Network Controller UI.

Attention

- 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.
- Crosswork Network Controller does not manage the backups. It is the operator's responsibility to periodically delete old backups from the target server to make room for future backups.
- Crosswork Network Controller backup process depends on having SCP access to a server with sufficient storage space. The storage required for each backup will vary based on your cluster size, applications in the cluster, and scale requirements.
- The time taken for the backup or restore processes will vary based on the type of backup, your cluster size, and the applications in the cluster.
- If you want to include NSO data in the Crosswork Network Controller backup process, follow the instructions given in Backup Crosswork Network Controller with NSO, on page 16 instead of the instructions in this topic.

Before you begin

Before you begin, ensure that you have:

- The hostname or IP address and the port number of the secure SCP server. Ensure that the server has sufficient storage available.
- A file path on the SCP server, to use as the destination for your backup files.
- User credentials for an account with file read and write permissions to the remote path on the destination SCP server.
- Noted the build version of the installed applications. Before performing a data restore, you must install the exact versions of those applications. Any mismatch in build versions can result in data loss and failure of the data restore job.

When creating or restoring backups for a Crosswork Network Controller cluster, follow these guidelines:

- 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.
- 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 same platform image for disaster restore as was used for creating the backup. Different software versions are not compatible for disaster restores.
- 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.
- 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).
- Delete older backups to save space on the backup server, though they 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.
- 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. For more information, see Import Cluster Inventory, on page 29.
- 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. For information on how to import the certificate, see Change Current System Settings, on page 397.

Step 1 **Configure an SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 2 **Create a backup:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Data Backup** to display the **Data Backup** dialog box with the destination server details pre-filled.
c) Provide a relevant name for the backup in the **Job Name** field.
d) If you want to create the backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
e) Uncheck the **Backup NSO** checkbox if you don't want to include Cisco NSO data in the backup.

Note To select the **Backup NSO** option, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail.

f) Complete the remaining fields as needed.

If you want to specify a different remote server upload destination: Edit the pre-filled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

g) (Optional) Click **Verify Backup Readiness** to verify that Crosswork Network Controller has enough free resources to complete the backup. If the check is successful, Crosswork Network Controller displays a warning about the time-consuming nature of the operation. Click **OK** to continue.
h) Click **Start Backup** to start the backup operation. Crosswork Network Controller creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.
i) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

j) *If the backup fails during upload to the remote server:* In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

Note The upload can fail due to multiple problems such as incorrect credentials, invalid destination directory, or lack of space in server. Investigate the problem and fix it (for example, clean old backups to free up space or use the **Destination** button to specify a different remote server and path) before clicking the **Upload backup** button.

Step 3 **To restore from a backup file:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) In the **Backup and Restore Job Sets** table, select the data backup file to be used for the restore. The **Job Details** panel shows information about the selected backup file.
c) With the backup file selected, click the **Data Restore** button shown on the **Job Details** panel to start the restore operation. Crosswork Network Controller creates the corresponding restore job set and adds it to the job list.

To view the progress of the restore operation, click the link to the progress dashboard.

Attention If the MDT collection jobs are deleted after a backup, the restore operation will fail to recover the MDT collection tasks. The MDT collection tasks will be in an error state as the associate devices will not have the required configurations.

This situation can be rectified using any ONE of the following actions:

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

Restore Crosswork Network Controller After a Disaster

A disaster recovery is a restore operation used after a natural or human-caused disaster destroys a Cisco Crosswork cluster. First, deploy a new cluster by following the instructions in the *Cisco Crosswork Network Controller 7.0 Installation Guide*.

Note If your cluster has only one malfunctioning hybrid node or one or more malfunctioning worker nodes, do not perform a disaster recovery. Instead, use cluster management features to redeploy or replace these nodes. If more than one hybrid node is malfunctioning, the system will not be functional. Replacing or rebooting the failed hybrid nodes may not guarantee recovery. In this case, deploy a new cluster and recover the entire system using a recent backup from the old cluster. For more information, see the Manage the Crosswork Cluster, on page 23 chapter in this guide.

To perform a disaster recovery:

Before you begin

Before performing a Data Disaster Restore, ensure the following:

- Obtain the full name of the backup file you want to use from the SCP backup server. Typically, this will be the most recent backup file you have created. Crosswork Network Controller backup filenames typically follow this format:

  `backup_`*`JobName`*`_`*`CWVersion`*`_`*`TimeStamp`*`.tar`

  - *JobName* is the user-entered name of the backup job.
  - *CWVersion* is the Crosswork Network Controller platform version of the backed-up system.
  - *TimeStamp* is the date and time when Crosswork Network Controller created the backup file.

  For example: `backup_Wednesday_4-0_2021-02-31-12-00.tar`.

- Install the exact versions of the applications that were present in your old Crosswork Network Controller cluster when the data backup was made. Any version mismatch can lead to data loss and restore job failure.

- The new Crosswork Network Controller cluster must use the same IP addresses as the original cluster where the backup was taken. This is crucial because internal certificates rely on these IP addresses.
- The new cluster must have the same number and types of nodes as the original cluster.
- Use the same Crosswork Network Controller software image that was used when creating the backup. You cannot restore the cluster using a backup created with a different software version.
- Keep your backups up-to-date to ensure you can recover the system's true state as it existed before the disaster. If you have installed new applications or patches since your last backup, take another backup.
- If the disaster recovery fails, contact Cisco Customer Experience for assistance.
- Smart licensing registration for Crosswork Network Controller applications is not restored during a disaster restore operation and must be registered again.

Step 1 From the main menu of the newly deployed cluster, choose **Administration** > **Backup and Restore**.

Step 2 Click **Actions** > **Data Disaster Restore** to display the **Data Disaster Restore** dialog box with the remote server details pre-filled.

Step 3 In the **Backup File Name** field, enter the file name of the backup from which you want to restore.

Step 4 Click **Start Restore** to initiate the recovery operation.

To view the progress of the operation, click the link to the progress dashboard.

Crosswork Data Gateway Disaster Recovery Scenarios

This section explains the various scenarios to restore the data gateways after Cisco Crosswork Network Controller recovers from a disaster.

The Crosswork Network Controller disaster recovery process automatically restores the data gateways in the network. You only need to follow additional procedures if the data gateway VMs have been deleted from Crosswork Network Controller.

- Crosswork Data Gateway Disaster Recovery with High Availability, on page 12: All active and standby the data gateway VMs in a pool have the **Operational state** as **Error**.
- Crosswork Data Gateway Disaster Recovery without High Availability, on page 14: A pool that has only one data gateway VM, or a pool that has multiple active data gateway VMs in the **Error** state without any standby VMs.

Crosswork Data Gateway Disaster Recovery with High Availability

Follow these steps to restore a data gateway pool with active and standby Data Gateway VMs in the **Error** state. For the purpose of these instructions, we use a pool with one active and one standby VM.

Before you begin

Ensure that you have completed the Cisco Crosswork disaster recovery operation before you proceed with this procedure. This implies that the Crosswork backed up data before the disaster is restored and all the Crosswork's pods are healthy and operational.

Note Do no redeploy the data gateways before verifying that Crosswork is fully restored and all the pods are healthy.

Step 1 Install new data gateway VMs with same information (profile, hostname, management interface) as the VMs in the pool prior to the disaster.

The newly installed data gateway VMs have the operational state as **Error** since Cisco Crosswork's disaster recovery process restores data from the older VMs.

Step 2 Log in to Cisco Crosswork.

Step 3 Navigate to **Administration** > **Data Gateway Management** > **Pools**.

Step 4 Select and edit the pool to remove (unassign) the standby VM from the pool. See Edit or Delete a Crosswork Data Gateway Pool, on page 69

Step 5 Change the **Administration State** of the standby VM to the **Maintenance** mode. See Change the Administration State of Crosswork Data Gateway Instance, on page 73.

Note If the Data Gateway is redeployed without moving it to the **Maintenance** mode, the enrollment with Crosswork fails and the following errors appear in the logs:

In the dg-manager logs:

```
time="2023-03-18 06:44:54.305973" level=error msg="[re-installing dg requires admin state to
be in maintenance mode and role "+\n"to be unassigned]" tag=ROBOT_dg-manager_dg-manager-0 - DG
 re-installed
```

In the controller-gateway logs:

```
2021-02-11T21:25:32.373 ERROR - Received Error from AutoEnroll Challenge Token Response call
re-installing dg requires admin state to be in maintenance mode and role to be unassigned
2021-02-11T21:25:32.373 ERROR - Error while posting sendTokenResponse re-installing dg requires
 admin state to be in maintenance mode and role to be unassigned
```

To rectify the problem, you can switch the Data Gateway to the **Maintenance** mode or manually re-enroll the gateway. For more information, Re-enroll Crosswork Data 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 to 7 to restore the (now) standby VM that has the **Operational State** as **Error**.

Step 8 Verify the following:

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

Crosswork Data Gateway Disaster Recovery without High Availability

In case of a disaster, you can restore the data gateway VM without high availability by using one of the following methods (**Steps**):

- Replace the old VM with a newly installed VM that is installed with the same information as the old VM
- Detach devices or move devices to another Data Gateway in the network
- Add a standby VM to the pool (install an additional VM and add it as a standby in the pool)

Before you begin

Ensure that you have completed the Cisco Crosswork disaster recovery operation before you proceed with this procedure. All information about the data gateway VMs and pools will be available in Cisco Crosswork once the Crosswork disaster recovery process is complete.

Step 1 **Replace the old VM with a newly installed VM that is installed with the same information as the old VM**

a) Log in to Cisco Crosswork.
b) Navigate to **Administration** > **Data Gateway Management** > **Data gateways**.
c) Delete the existing pool.
d) Change the **Administration State** of the VM to the **Maintenance** mode. See Change the Administration State of Crosswork Data Gateway Instance, on page 73.
e) Install a new data gateway VM with the same information as the older VM.
f) Change the **Administration State** of the VM to **Up** from **Maintenance**.

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

g) Create a new pool with the same name as the older pool and add the VM to the pool.

Verify the data gateway has the **Operational State** as **Up**

h) Attach devices to the data gateway. See Attach Devices to a Crosswork Data Gateway, on page 63.
i) Verify that collection jobs are running as expected.

Step 2 **Detach devices or move devices to another data gateway in the network**

a) Log in to Cisco Crosswork.
b) Navigate to **Administration** > **Data Gateway Management** > **Data gateways**.
c) Detach devices from the VM or move devices to another data gateway that is operationally **Up**. See Manage Crosswork Data Gateway Device Assignments, on page 71.
d) Delete the existing pool.

This step will not unassign the VM from the pool. The VM will continue to show as assigned to the pool.

e) Change the **Administration State** of the VM to the **Maintenance** mode. See Change the Administration State of Crosswork Data Gateway Instance, on page 73.
f) Reboot the VM. With this step, the VM is unassigned from the pool.

Wait for about 5 minutes. The VM enrolls with Cisco Crosswork automatically. Verify that the VM is in the administratively UP and is in the **Not Ready** state.

Note You can also manually re-enroll the VM with Cisco Crosswork from the Interactive Console of the data gateway VM. See Re-enroll Crosswork Data Gateway, on page 418.

g) Create a new pool with the same name as the older pool and add the VM to the pool.
h) Verify the data gateway has the **Operational State** as **Up**.
i) Attach devices or move devices back to this data gateway. See Manage Crosswork Data Gateway Device Assignments, on page 71.
j) Verify that collection jobs are running as expected.

Step 3 **Add a standby VM to the pool (install an additional VM and add it as a standby in the pool)**

Note The following steps list the procedure to restore a pool that has a single active VM in the **Error** state. To restore multiple active VMs in a pool in the **Error** state without any standby VMs, ensure that you add an additonal VM for each active VM in the pool.

a) Install a new data gateway VM.
b) Log in to Cisco Crosswork.
c) Navigate to **Administration** > **Data Gateway Management** > **Pools**.
d) Select and edit the pool to add the newly installed VM to the pool. See Edit or Delete a Crosswork Data Gateway Pool, on page 69

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

e) Edit the pool and remove the (now) standby VM from the pool.
f) Change the **Administration state** of the standby VM to **Maintenance** mode. See Change the Administration State of Crosswork Data Gateway Instance, on page 73.

   Wait for about 5 minutes. The VM enrolls with Cisco Crosswork automatically. Verify that the VM is operationally UP and is in the **Not Ready** state.

   Note You can also manually re-enroll the VM with Cisco Crosswork from the Interactive Console of the data gateway VM. See Re-enroll Crosswork Data Gateway, on page 418.

g) Edit the pool again and add the standby VM to the pool.
h) Verify the data gateway is operationally **Up** and the pool has an active and standby VM.
i) Verify the following:

   • Devices are attached to active VM in the pool.

   • Collection jobs are running as expected.

Resolve SR-TE Policies and RSVP-TE Tunnels

Orphaned TE policies are any PCE initiated SR-TE policies (SRv6, SR-MPLS, and Tree-SID) or RSVP-TE tunnels that were created within Crosswork and *after* the last cluster data synchronization. After a switchover in a High Availability setup, Crosswork automatically checks for any orphaned TE policies. Orphaned policies/tunnels may also happen after a backup/restore operation. You can view policy details but not modify them since they were not included in the last data synchronization. Crosswork will display an alarm when it finds orphan TE policies (**Alerts > Alarms and Events**).

Crosswork provides APIs to help clear these orphans. To get a list of orphan SR-TE policies or RSVP-TE tunnels, use **cisco-crosswork-optimization-engine-sr-policy-operations:sr-datalist-oper** or **cisco-crosswork-optimization-engine-rsvp-te-tunnel-operations:rsvp-te-datalist-oper** where **is-orphan=True** and default action is GET. To make the orphans manageable again, use a SAVE action for

the corresponding URL per policy type. For more information, see API documentation on Devnet (**Crosswork Optimization Engine APIs > *release-id* Release APIs**).

Backup Crosswork Network Controller with NSO

You can create a backup of just the Crosswork Network Controller or include a copy of the NSO CDB (the default data store for configuration data in NSO). To back up the CDB, your Crosswork Network Controller user account must meet specific requirements detailed in the Add Cisco NSO Providers, on page 244 section.

Note While the backup can be automated (as described), the restore of the NSO CDB is a manual process. For detailed instructions, see Restore Crosswork Network Controller with NSO, on page 17).

Before you begin

Before you begin, ensure:

- You have the hostname or IP address and the port number of a secure SCP server.
- You have a file path on the SCP server, to use as the destination for your backup files.
- You have the user credentials for an account with read and write permissions to the storage folder on the destination SCP server.
- To select the **Backup NSO** option, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail.
- Ensure the NSO provider, the Crosswork Network Controller credential profile associated with the NSO provider, and the NSO server meet the following prerequisites:
  - Ensure that SSH is enabled on the NSO provider configuration.
  - The user ID associated with the SSH connectivity type in the credential profile assigned to the NSO provider has sudo permissions.
  - The NSO server has NCT (NSO Cluster Tools) installed, and the user in the credential profile for the NSO provider can execute `nct` commands.
  - The user in the NSO provider's credential profile has full access to the NSO server's backup folder and the files in it. This requirement usually means full read and write access to the NSO server's `/var/opt/ncs/backups/` folder.

Failure to meet any of these NSO requirements means that all or part of the backup job will fail.

In addition to these special requirements, the normal guidelines for backups discussed in Manage Crosswork Network Controller Backup and Restore, on page 8 also apply to backups containing NSO data.

Step 1 **Configure an SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 2 **Create the backups of Crosswork Network Controller and NSO:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Actions** > **Backup** to display the **Backup** dialog box with the destination server details prefilled.
c) Provide a relevant name for the backup in the **Job Name** field.
d) If you want to create the backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
e) Leave the **Backup NSO** check box checked.
f) Complete the remaining fields as needed.

   If you want to use a different remote server upload destination, click **cancel**, then select the destination tab and edit the values.

g) Click **Start Backup** to start the backup operation. Crosswork Network Controller creates the corresponding backup job set adds it to the job list, and begins processing the backup. The Job Details pane reports the status of each backup step as it is completed.
h) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup Restore Job Sets** table. Then click on the job set you want.

   The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

i) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

   If the upload failed due to problems with the remote server, use the **Destination** button to specify a different remote server and path before clicking **Upload backup**.

Restore Crosswork Network Controller with NSO

When you restore a Crosswork Network Controller cluster and its associated NSO from a backup, follow these guidelines:

- We recommend performing restore operations during a scheduled maintenance window only. Users should not attempt to access Crosswork Network Controller or NSO while these operations are running. The restore operations are lengthy and will pause other Crosswork Network Controller applications until they are complete. NSO must be completely stopped during restore operation.

Note Restore from the NSO backup file is a manual process, currently.

Before you begin

Get the full name of the backup file you want to restore from the SCP server. This file will contain both the Crosswork Network Controller and NSO backups. Backup filenames have the following format:

`backup_`*`JobName_CWVersion_TimeStamp`*`.tar`

Where:

- *JobName* is the user-entered name of the backup job.

- *CWVersion* is the Crosswork Network Controller version of the backed-up system.
- *TimeStamp* is the date and time when Crosswork Network Controller created the backup file.

For example: `backup_Wed_4-0_2021-02-31-12-00.tar`.

Step 1 Log in (if needed) to the remote SCP backup server. Using the Linux command line, access the backup destination directory and find the backup file containing NSO information that you want to restore. For example:

```
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_4-0_2021-02-31-12-00.tar
```

Step 2 Use `tar -xvf` to extract the NSO backup from the Crosswork Network Controller backup file in the destination folder. For example:

```
[root@localhost~]# tar -xvf backup_Wed_4-0_2021-02-31-12-00.tar
...
[root@localhost~]# ls -ltr
-rw-rw-r--. 1 root root 8265938605 backup_Wed_4-0_2021-02-31-12-00.tar
-rw-r--r--. 1 root root 8267798605 468c4715-ea09-4c2b-905e-98999d.tar
```

Step 3 Un-tar the NSO backup file in the destination folder. You will see NSO files being extracted to a folder structure under `/nso/`*`ProviderName`*`/`, where `/nso/`*`ProviderName`*`/` is the name of the NSO provider as configured in Crosswork Network Controller. 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. In the example in the previous step, the file name is highlighted.

Step 5 Log in to NSO as a user with root privileges and access the command line. Then copy or move the generated NSO backup file from the SCP server to the specified restore path location of the NSO cluster. For example:

```
[root@localhost nsol21]# 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 You can perform NSO restore operations only while NSO is not running. At the NSO cluster command line, run the following command to stop NSO:

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

Step 7 Once NCS has stopped, start the restore operation using the following command and the name of the generated NSO backup file. For example:

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

If you have trouble running this command, first give yourself `sudo su` permission.

Step 8 Once the restore completes, restart NSO using the following command. This command may take a few minutes to complete.

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

Step 9 Once you have restored both Crosswork Network Controller and NSO clusters from backups, re-add the NSO provider to Crosswork Network Controller.

Migrate Data Using Backup and Restore

Using data migration backup and restore is a prerequisite when upgrading your Crosswork Network Controller installation to a new software version, or moving your existing data to a new installation.

Follow these guidelines whenever you create a data migration backup:

- Ensure that you have configured a destination SCP server to store the data migration files. This configuration is a one-time activity.
- Both the Crosswork Network Controller cluster and the SCP server must be in the same IP environment. For example: If Crosswork Network Controller is communicating over IPv6, so must the backup server.
- We recommend that you create a data migration backup only when upgrading your Crosswork Network Controller installation, and that you do so during a scheduled upgrade window only. Users shouldn't attempt to access Crosswork Network Controller while the data migration backup or restore operations are running.
- Ensure that you capture a screenshot of the data gateways to keep a record of the assigned IP addresses and names. You need this information when you deploy the new data gateways.

Before you begin

Ensure that you have:

- 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 destination SCP server.

Step 1 **Configure a SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 2 **Create a backup:**

a) Log in as an administrator to the Crosswork Network Controller installation whose data you want to migrate to another installation.
b) From the main menu, choose **Administration** > **Backup and Restore**.
c) Click **Actions** > **Data Backup** to display the **Data Backup** dialog box with the destination server details prefilled.
d) Provide a relevant name for the backup in the **Job Name** field.
e) If you want to create the backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
f) Complete the remaining fields as needed.

If you want to specify a different remote server upload destination: Edit the pre-filled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

g) Click **Start Backup** to start the backup operation. Crosswork Network Controller creates the corresponding backup job set and adds it to the **Backup and Restore Job Sets** table. The Job Details panel reports the status of each backup step as it is completed.

h) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

i) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

If the upload failed due to problems with the remote server, use the **Destination** button to specify a different remote server and path before clicking **Upload backup**.

Step 3 **Migrate the backup to the new installation:**

a) Log in as an administrator on the Crosswork Network Controller installation to which you want to migrate data from the backup.

b) From the main menu, choose **Administration** > **Backup and Restore**.

c) Click **Actions** > **Data Migration** to display the **Data Migration** dialog box with the remote server details pre-filled.

d) In the **Backup File Name** field, enter the file name of the backup from which you want to restore.

e) Click **Start Migration** to initiate the data migration. Crosswork Network Controllercreates the corresponding migration job set and adds it to the job list.

To view the progress of the data migration operation, click the link to the progress dashboard.

Step 4 **Deploy Crosswork Data Gateway:**

a. After the migration is complete, log out from the Crosswork UI and log in again to the UI using https://<new_crosswork_ip>:30603.

The **Action to be taken** pop-up appears with the message **Please Acknowledge once redeploy of the CDGs is done**.

b. In the **Action to be taken** pop-up, click **Cancel**.

c. Delete the old data gateway VMs and install new gateways. Ensure that they have the identical IPs and names as the previous gateway VMs.

d. Verify that the deployment of the data gateway is complete, and the gateway is registered with Crosswork Network Controller.

e. Verify that the data gateway is in the same state as it was before the upgrade by choosing **Administration > Data Gateway Management > Virtual Machines**. The **Operation** and **Administration** state of the data gateways should be UP.

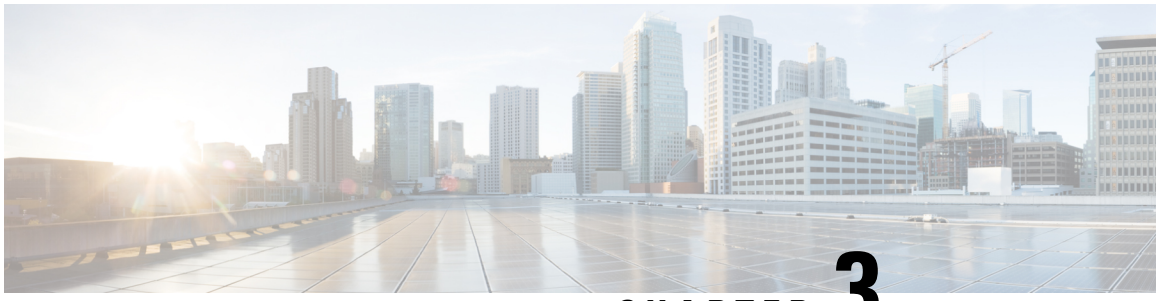
f. After all the data gateways are active, navigate to **Administration > Data Gateway Management > Pools** page to verify the successful migration of all pools from the previous cluster version and ensure that data gateways are automatically enrolled with Crosswork Network Controller.

g. Log out from the Crosswork UI and log in back to the UI using https://<new_crosswork_ip>:30603. The **Action to be taken** pop-up appears.

Note Do not click on the browser history links that have a child path to access the UI. This prevents the **Action taken** pop-up from appearing.

h. In the pop-up, click **Acknowledge**. With this step, the migration should be complete.

i. If the NSO is set to the read-only mode, disable it.



CHAPTER 3

Manage the Crosswork Cluster

This section contains the following topics:

Cluster Management Overview

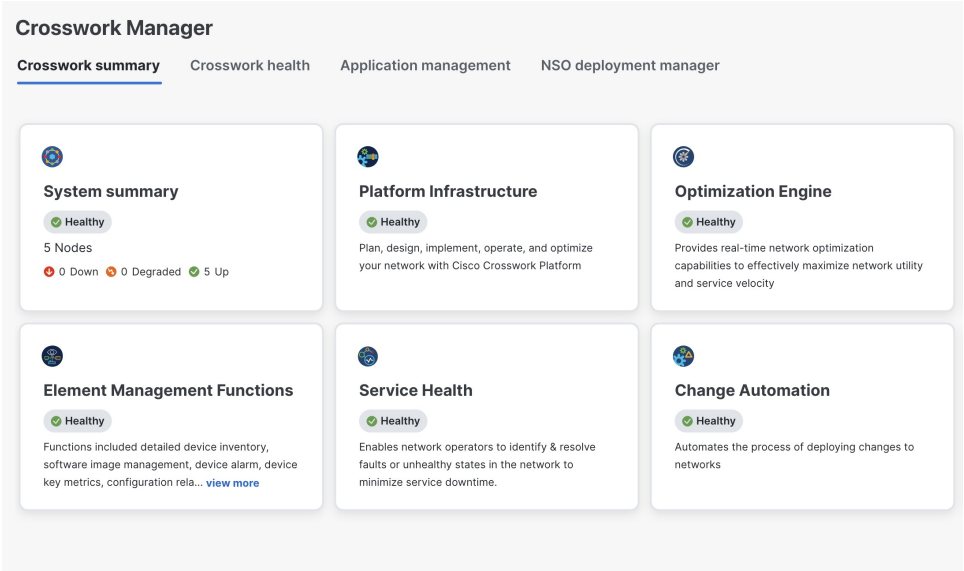
The Cisco Crosswork platform uses a cluster architecture. The cluster distributes platform services across a unified group of virtual machine (VM) hosts, called nodes. The underlying software architecture distributes processing and traffic loads across the nodes automatically and dynamically. This architecture helps Cisco Crosswork respond to how you actually use the system, allowing it to perform in a scalable, highly available, and extensible manner.

A single Crosswork cluster consists of a minimum of three nodes, all operating in a hybrid configuration. These three hybrid nodes are mandatory for all Cisco Crosswork deployments. If you have more demanding scale requirements, you can add up to two worker nodes. For more information, see Deploy New Cluster Nodes, on page 29.

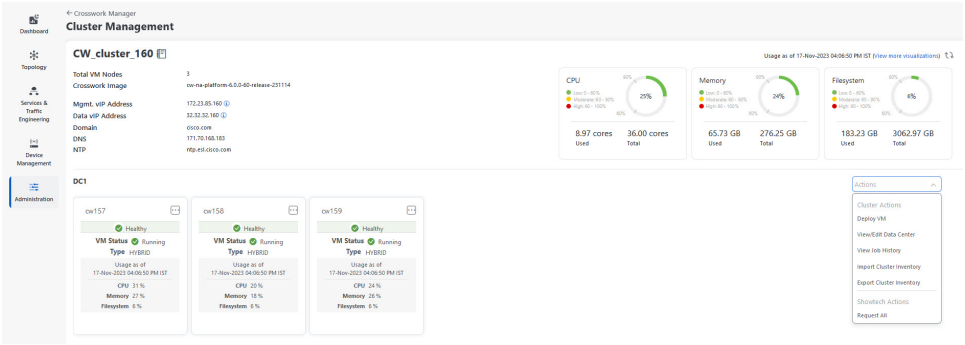
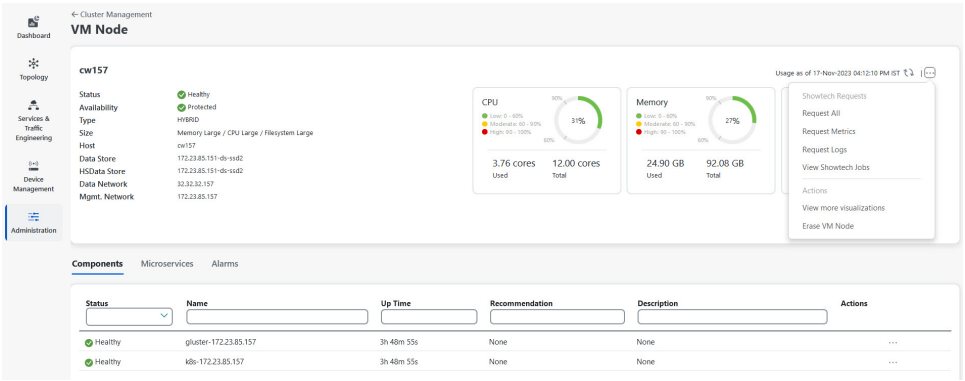
Only users assigned to the admin role or a role with proper permissions will have access to all of the cluster configuration.

Table 4: Cluster Overview

Action	Description
Navigation	Use the **Crosswork Manager** window to check the health of the cluster. To display this window, from the main menu, choose **Administration** > **Crosswork Manager**.

Action	Description
Crosswork Summary window	The **Crosswork Manager** window gives you summary information about the status of the nodes, the Platform Infrastructure, and the applications you have installed. ***Figure 1: Crosswork Manager (cluster deployment)*** 

Action	Description
Cluster Management window	

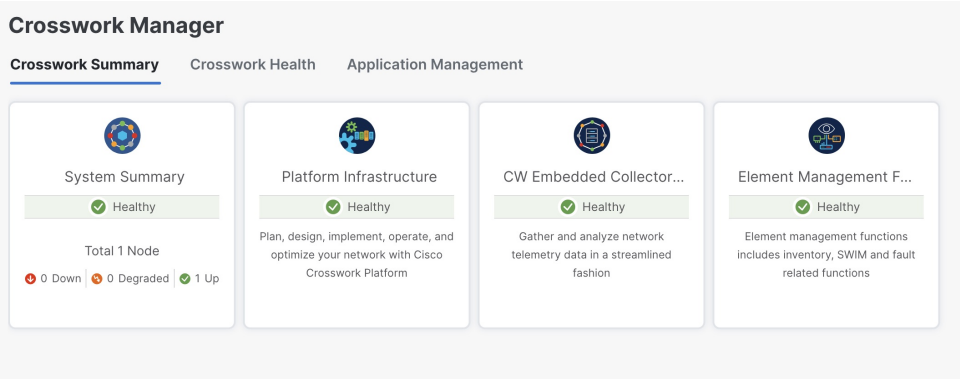
Action	Description
	Note Applicable only when Crosswork is deployed as a cluster. Click on the **System Summary** tile to see the details of the nodes in the cluster. ***Figure 2: Cluster Management Window***  The top left section of the window provides details about the cluster while the top right provides details about overall cluster resource consumption. The bottom section breaks down the resource utilization by node, with a separate detail tile for each node. The window shows other details, including the IP addresses in use, whether each node is a hybrid or worker, and so on. On the top-right corner, click the **View more visualizations** link to Visually Monitor System Functions in Real Time, on page 369. To see details for a specific node, click ⋯ on the tile of the node, and choose **View Details**. The VM Node window displays the node details, including the list of components, microservices, and alarms running on the node. • To request metrics or logs, click ⋯ under the **Action** column, and select the relevant option. • To restart a microservice, click ⋯ under the **Action** column, and choose **Restart**. ***Figure 3: Node details*** 

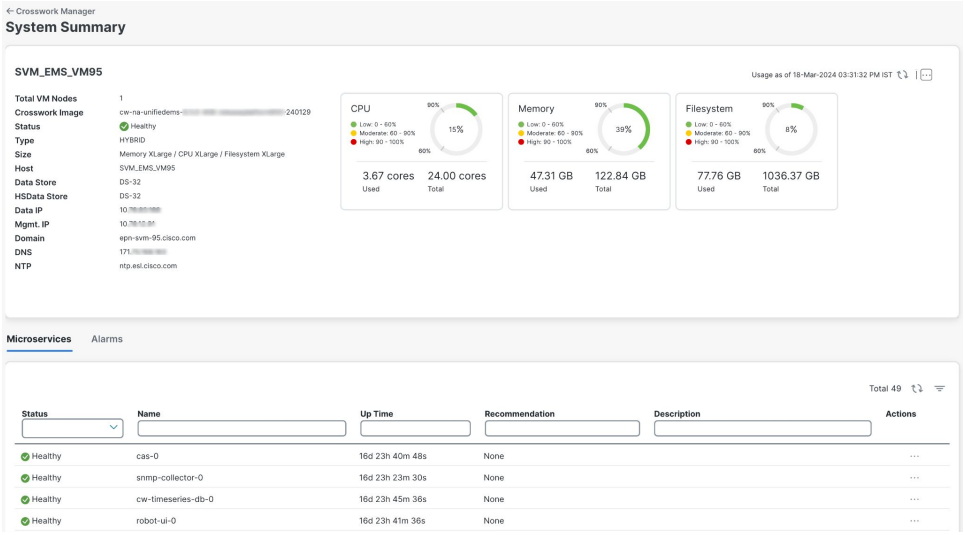
Action	Description
	For information on how to use the **Crosswork Health** tab, see Monitor Platform Infrastructure and Application Health, on page 368.

Single VM based Crosswork Network Controller

Starting with 7.0 release, Crosswork can also be deployed on a single VM that delivers all the functionality with a limited capacity for devices. When deployed as a single VM, all the functions run on a single machine with limited redundancy.

Table 5: Single VM overview

Action	Description
Navigation	Use the **Crosswork Manager** window to check the health of the cluster. To display this window, from the main menu, choose **Administration** > **Crosswork Manager**.
Crosswork Summary window	The **Crosswork Manager** window gives you summary information about the status of the nodes, the Platform Infrastructure, and the applications you have installed. ***Figure 4: Crosswork Summary (single VM deployment)*** 

Action	Description
System Summary window	**Note** Applicable only when Crosswork is deployed on a single VM. Click on the **System Summary** tile to see the VM details. ***Figure 5: VM details*** 

Note

- If one of the hybrid nodes is faulty, along with one or more worker nodes and applications, try the *Clean System Reboot* procedure described in Cluster System Recovery, on page 39.
- If more than one hybrid node is faulty, follow the *Redeploy and Recover* procedure described in Cluster System Recovery, on page 39.
- 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.

View and Edit Data Center Credentials

This section explains the procedure to view and edit the credentials for the data center (such as VMware vCenter) where Cisco Crosswork is deployed.

Before you begin

Ensure you have the current credentials for vCenter.

Note In case you have changed your password since Crosswork was originally deployed, you may need to update the stored credentials that Crosswork will use when deploying the new VM.

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.

Import Cluster Inventory

If you have installed your cluster manually using the vCenter UI (without the help of cluster installer tool), you must import an inventory file (.tfvars file) to Cisco Crosswork to reflect the details of your cluster. The inventory file contains information about the VMs in your cluster along with the data center parameters.

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

Note Please uncomment the "*OP_Status*" parameter while importing the cluster inventory file manually. If you fail to do this, the status of the VM will incorrectly appear as "Initializing" even after the VM becomes functional.

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 Cluster Inventory** to display the **Import Cluster Inventory** dialog box.

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 7.0 Installation Guide*.

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

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

Deploy New Cluster Nodes

As your network expands and you install additional Crosswork applications, it may become necessary to add more resources to handle the increasing workload. This topic explains how to deploy a new VM node.

The steps necessary to deploy a new node via the UI and the API are essentially the same. For details on using the API, see cluster APIs. This guide will only present the procedure for using the UI.

Important If you installed your cluster manually, you must import the cluster inventory file to Cisco Crosswork before you can deploy a new node. For more information, see Import Cluster Inventory, on page 29. The **Deploy VM** option will be disabled until you complete the import operation.

Before you begin

You must know the following:

- Details about the Cisco Crosswork network configuration, such as the management IP address.
- Details about the VMware host where you are deploying the new node, such as the data store and data VM interface IP address.
- The type of node you want to add. Your cluster can have a minimum of three hybrid nodes and up to two worker nodes.

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

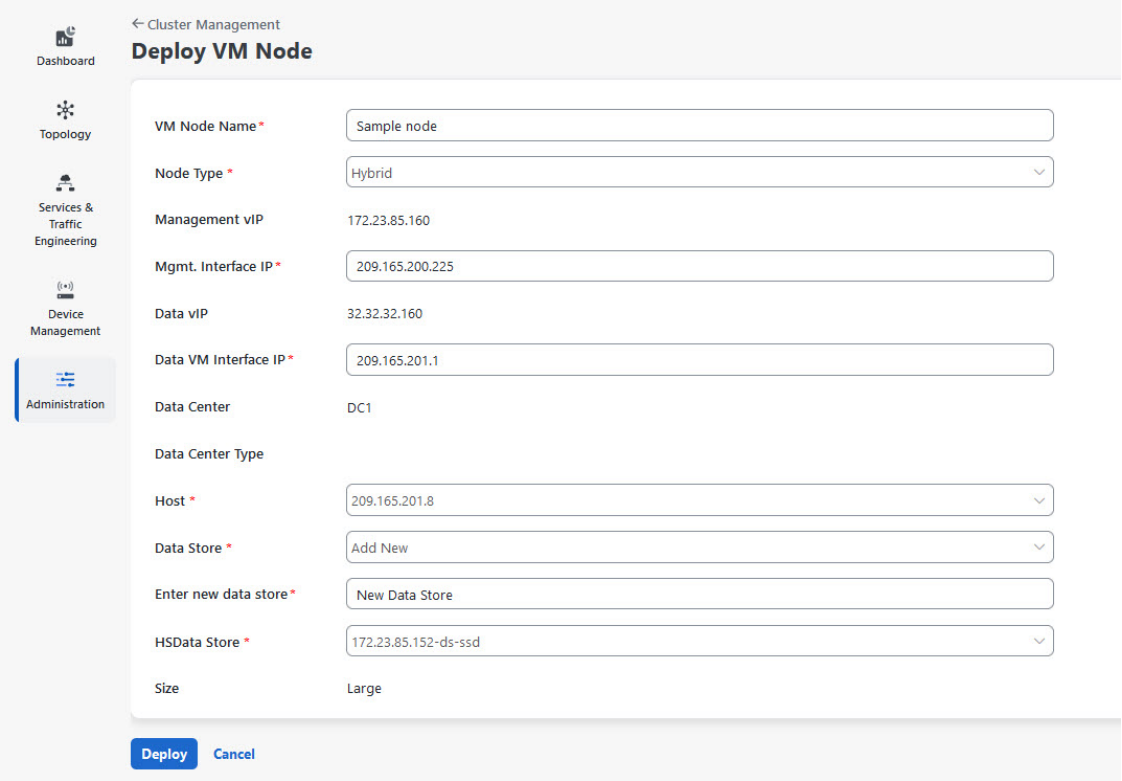
Step 2 On the **Crosswork Summary** tab, click the **System Summary** tile to display the **Cluster Management** window.

Note The **Crosswork Summary** window and the **Cluster Management** window display information about your cluster. While both windows display the status of the same cluster, there may be slight mismatches in the representation. This occurs because the **Crosswork Summary** window displays the node status based on Kubernetes, while the **Cluster Management** window also considers the node status in the data center.

An example of this mismatch is when a worker node deployment fails in the Crosswork UI due to insufficient data center resources. In this case, the status of the failed worker node is displayed as "degraded" in the **Cluster Management** window, while the same status appears as "down" in the **Crosswork Summary** window.

Step 3 Choose **Actions** > **Deploy VM** to display the **Deploy VM Node** window.

Figure 6: Deploy VM Node Window



Step 4 Fill the relevant values in the fields provided.

Step 5 Click **Deploy**. The system starts to provision the new node in VMware. Cisco Crosswork adds a tile for the new node in the **Crosswork Manager** window. The tile displays the progress of the deployment.

You can monitor the node deployment status by choosing **Cluster Management** > **Actions** > **View Job History**, or from the VMware user interface.

If you have added the VM node using Cisco Crosswork APIs: On the newly added VM node tile, click ··· and choose **Deploy** to complete the operation.

Step 6 If this node was added to reduce the heavy load (running > 90%) on the existing nodes, you can rebalance the resources (see Rebalance Cluster Resources, on page 31 for details), or restart some processes to force the system to move them to the newly added node.

Rebalance Cluster Resources

As part of cluster management, Crosswork constantly monitors the resource utilization in each cluster node. If the CPU utilization in any of the nodes becomes high, Crosswork triggers a notification prompting you to take action. The alarm system has two levels. The first alarm triggers at around 70-80% usage, prompting you to plan for adding worker nodes (see Deploy New Cluster Nodes, on page 29). Ideally, new nodes should

be deployed before usage exceeds 90% to avoid performance issues. If you already have 5 or 6 nodes and still face resource shortages, please contact the Cisco Customer Experience team.

You can then use the **Rebalance** feature to reallocate the resources between the existing VM nodes in your cluster. Rebalancing is necessary if some nodes are busier than others. When a new worker is added, active workloads are not automatically moved to it, so rebalancing is required.

⚠

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.

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).

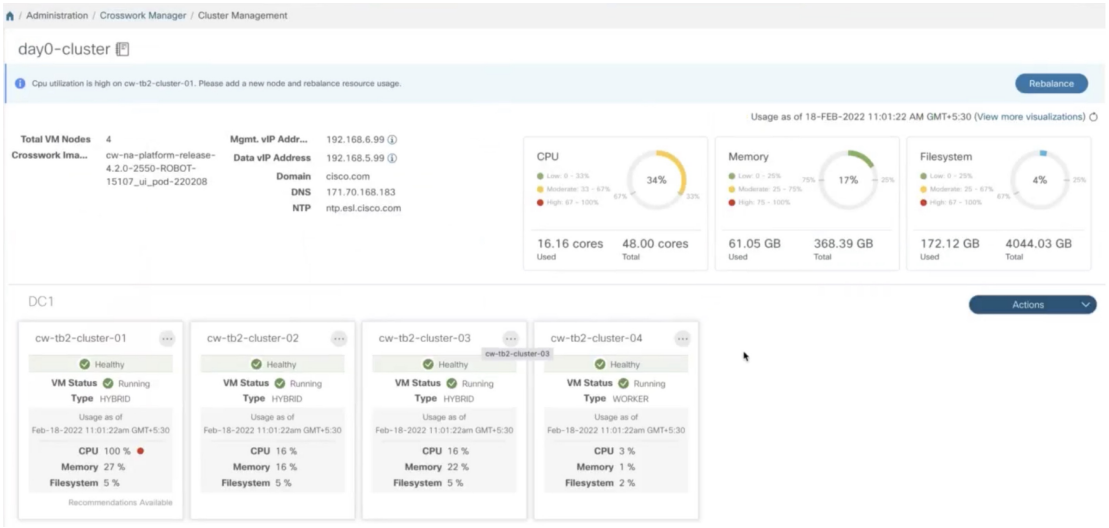
Step 1 From the main menu, choose **Administration** > **Crosswork Manager**.

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

For the sake of this procedure, a sample cluster (**day0-control**) with 3 hybrid nodes and 1 worker node is considered. The CPU utilization is high in one of the hybrid nodes (100% in **cw-tb2-cluster-01**). See the below image for more details.

The image below shows a cluster with four nodes and a banner recommending the user to add more worker nodes.

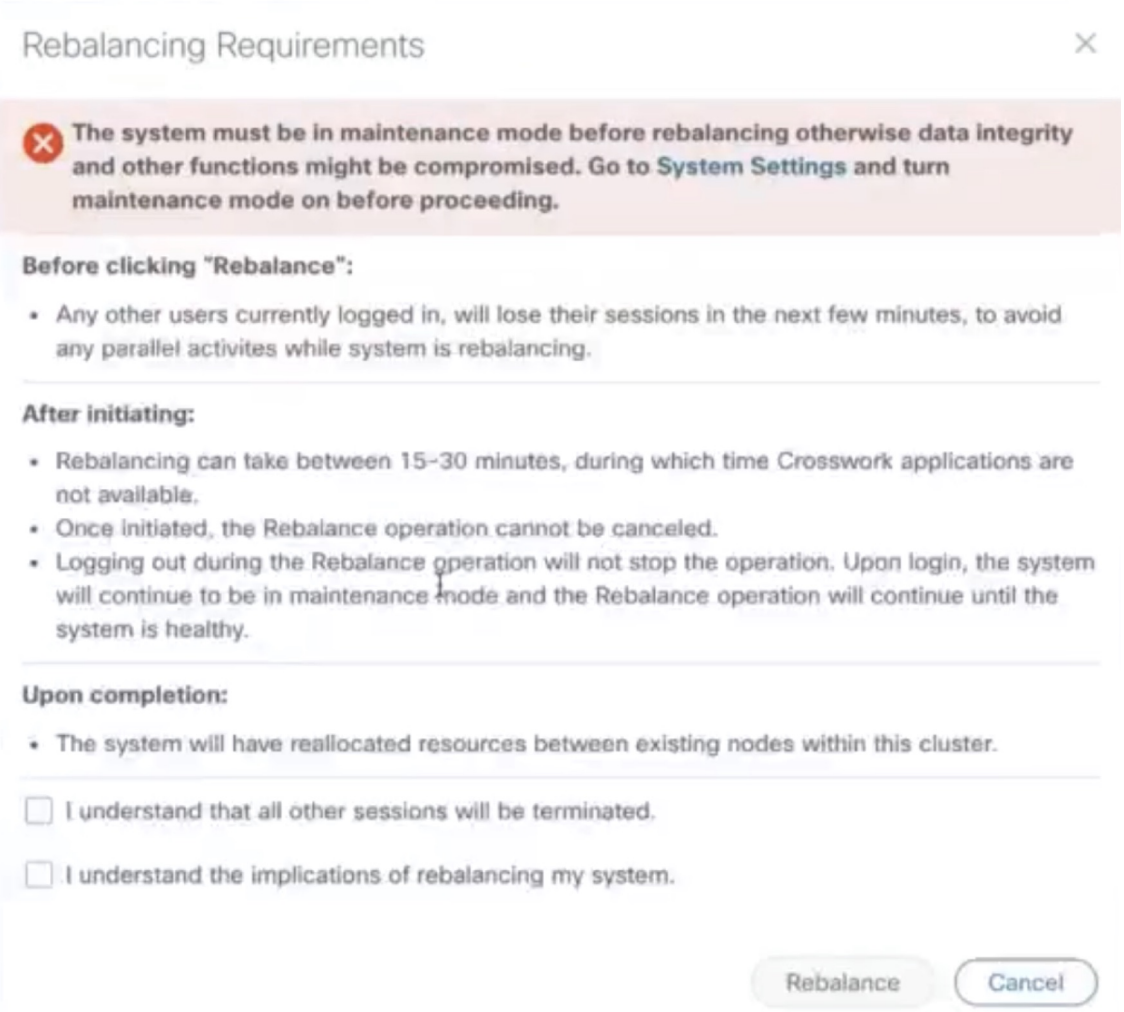
Figure 7: Rebalance notification



On the tile for the node, you can click ⋯ and choose **View Details** to see more details.

Step 3 Click **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.

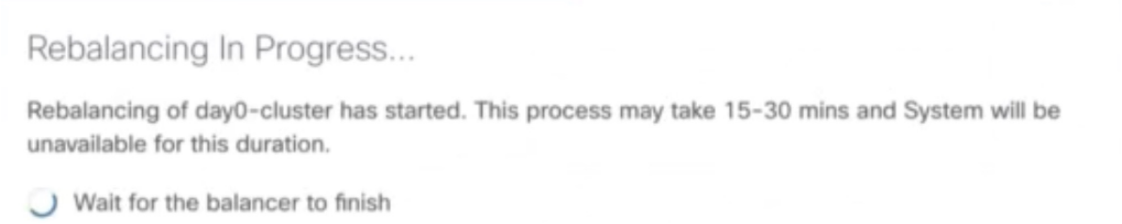
Figure 8: Rebalancing Requirements



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

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

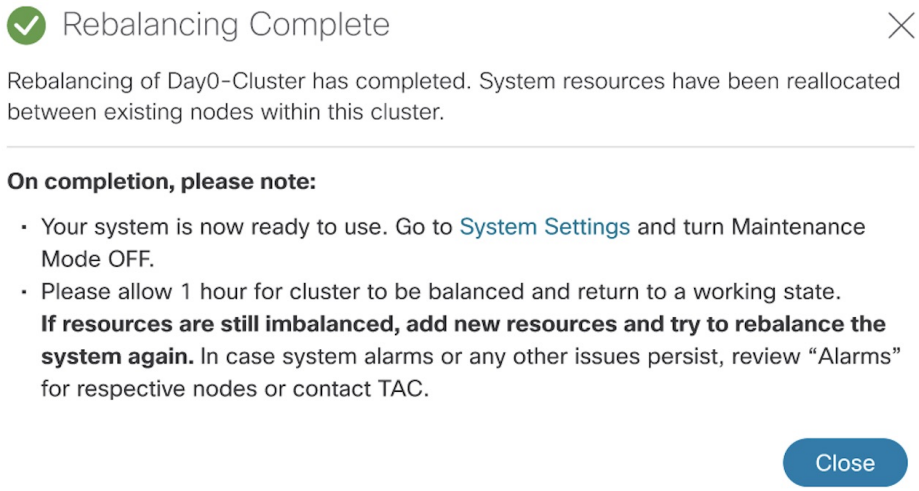
Figure 9: Rebalancing Status



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

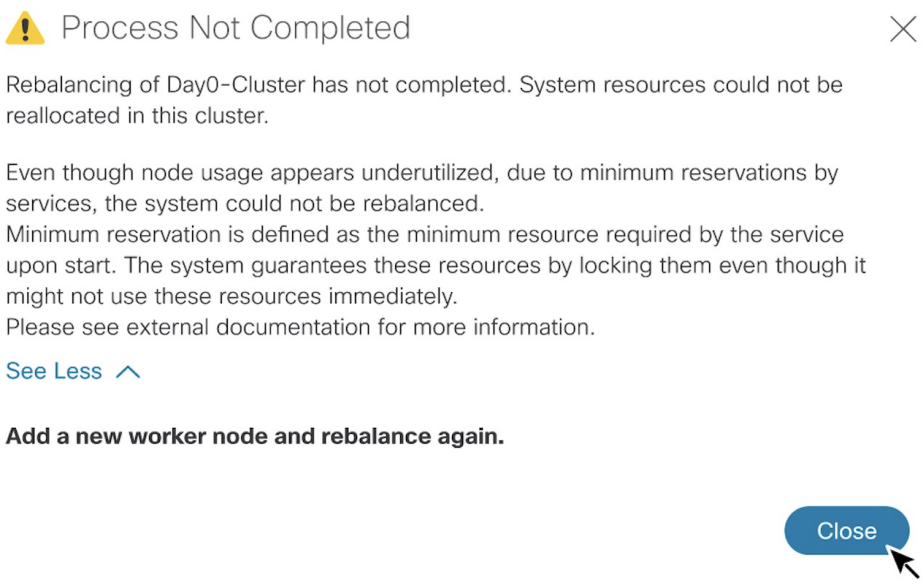
- **Success scenario:** A dialog box indicating successful rebalancing operation. Follow the instructions in the dialog box to proceed further.

  Figure 10: Rebalancing Result - Success



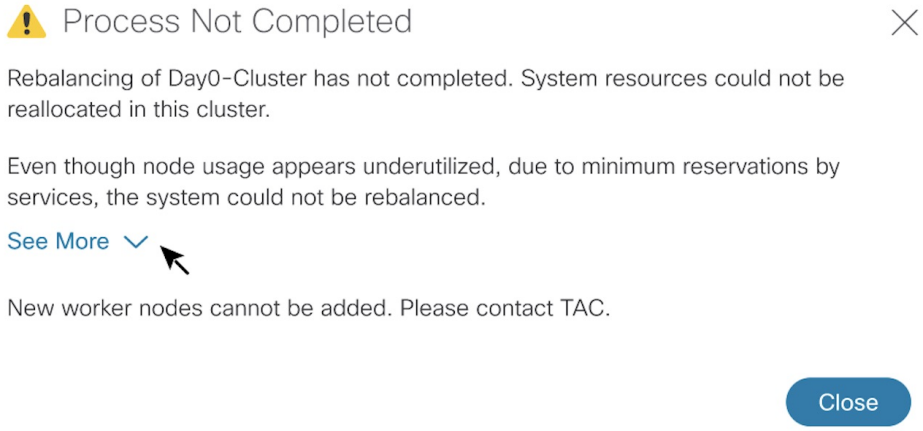
- **Failure scenario - scope available to add new worker nodes:** A dialog box indicating rebalancing failure is displayed. In this case, the system prompts you to add a new worker node and try the rebalance process again.

Figure 11: 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 nodes cannot be added.

Figure 12: Rebalancing Result - Add new Worker node



View Job History

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

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.

Export Cluster Inventory

Use the cluster inventory file to monitor and manage your Cisco Crosswork cluster.

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 Cluster Inventory**.

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

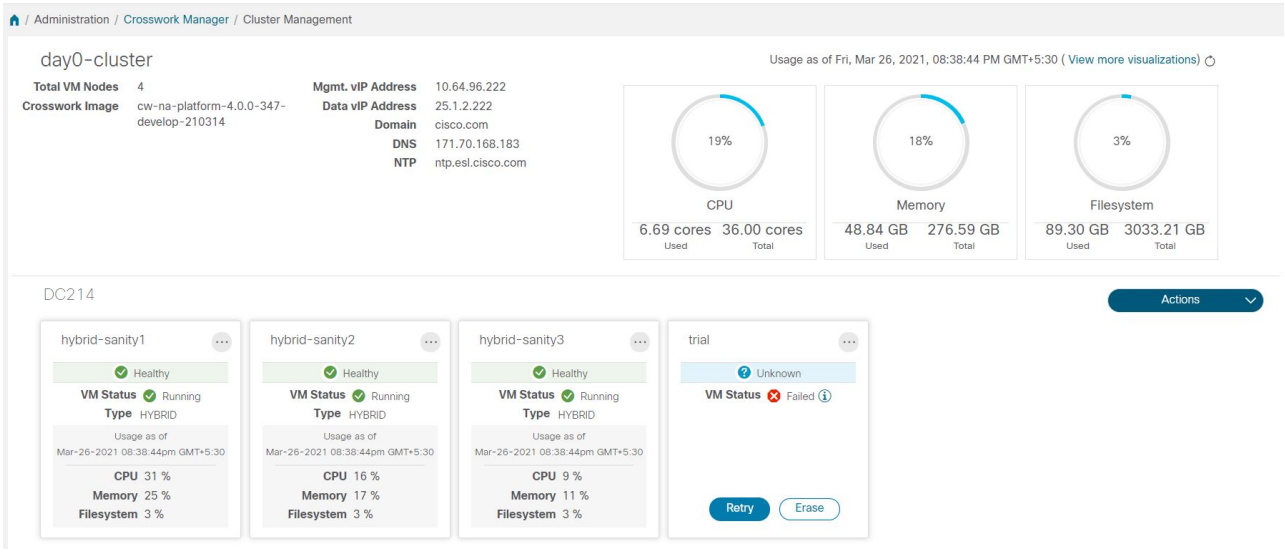
Retry Failed Nodes

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

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.

Figure 13: Cluster Management Window: Failed VM Deployment



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

Step 4 Provide corrected information in the fields provided.

Step 5 Click **Deploy**.

Erase Nodes

As an administrator, you can erase (that is, remove or delete) any **failed** or **healthy** node from the Cisco Crosswork cluster. Erasing a node removes the node reference from the Cisco Crosswork cluster and deletes it from the host VM.

The steps to erase a node are the same for both hybrid and worker nodes. However, the number and timing of erasure is different in each case:

- The system must maintain three operational hybrid nodes at all times. If one of the hybrid nodes stops functioning, Crosswork will attempt to compensate, however the system performance and protection against further failures will be severely impacted. In such cases, the faulty node is erased and a new hybrid node needs to be deployed to replace it.
- You can have up to two worker nodes. While you can erase all of them without consequences, we recommend that you erase and replace them one at a time.
- If you are still having trouble after taking these steps, contact the Cisco Customer Experience team for assistance.

Warning

- Erasing a node is a disruptive action and can block some processes until the action is completed. To minimize disruption, conduct this activity during a maintenance window only.
- Removing worker and hybrid nodes places extra workload on the remaining nodes and can impact system performance. You are encouraged to contact the Cisco Cisco Customer Experience team before removing nodes.
- While removing a Hybrid or Worker node, the Cisco Crosswork UI may become unreachable for 1-2 minutes, due to the relocation of the `robot-ui` pod to a new node.

Note For manual cluster installation, you must erase the VM from Crosswork UI and then delete the VM from the data center (e.g. vCenter).

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 On the tile for the node you want to remove, click ··· and select **Erase** to display the **Erase VM Node** dialog box .

Step 4 Click **Erase** again to confirm the action.

Note A removed node will continue to be visible in the Grafana dashboard as an entry with only historical data.

Manage Maintenance Mode Settings

Maintenance mode provides a means for shutting down the Crosswork system temporarily. The maintenance mode shutdown is graceful. Crosswork synchronizes all application data before the shutdown.

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

Attention

- Make a backup of your Crosswork cluster before enabling the maintenance mode.
- Notify other users that you intend to put the system in maintenance mode and give them a deadline to log out. The maintenance mode operation cannot be canceled once you initiate it.

Step 1 To put Crosswork in maintenance mode:

a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **Maintenance Mode**.

b) Drag the **Maintenance** slider to the right, or **On** position.
c) Crosswork warns you that it is about to initiate a shutdown. Click **Continue** to confirm your choice.

It can take several minutes for the system to enter maintenance mode. During that period, other users should not attempt to log in or use the Crosswork applications.

Note If you wish to reboot the cluster, wait for 5 minutes after system has entered maintenance mode in order to allow the Cisco Crosswork database to sync, before proceeding.

Step 2 To restart Crosswork from maintenance mode:

a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **Maintenance Mode**.
b) Drag the **Maintenance** slider to the left, or **Off** position.

It can take several minutes for the system to restart. During this period, users should not attempt to log in or use the Crosswork applications.

Note If a reboot or restore was performed when the system was previously put in maintenance mode, the system will boot up in the maintenance mode and you will be prompted with a popup window to toggle the maintenance mode off. If you do not see a prompt (even when the system was rebooted while in maintenance mode), you must toggle the maintenance mode on and off to allow the applications to function normally.

Cluster System Recovery

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.

When System Recovery Is Needed

Caution The methods explained in this topic may fail if you use a cluster profile consisting of only 3 hybrid VM nodes (and no worker nodes). The failure happens due to the lack of VM resiliency caused by the absence of worker nodes.

At some time during normal operations of your Cisco Crosswork cluster, you may find that you need to recover the entire system. This can be the result of one or more malfunctioning nodes, one or more malfunctioning services or applications, or a disaster that destroys the hosts for the entire cluster.

A functional cluster requires a minimum of three hybrid nodes. These hybrid nodes share the processing and traffic loads imposed by the core Cisco Crosswork management, orchestration, and infrastructure services. The hybrid nodes are highly available and able to redistribute processing loads among themselves, and to worker nodes, automatically.

The cluster can tolerate one hybrid node reboot (whether graceful or ungraceful). During the hybrid node reboot, the system is still functional, but degraded from an availability point of view. The system can tolerate

any number of failed worker nodes, but again, system availability is degraded until the worker nodes are restored.

Cisco Crosswork generates alarms when nodes, applications, or services are malfunctioning. If you are experiencing system faults, examine the alarm and check the health of the individual node, application, or service identified in the alarm. You can use the features described in Cluster Management Overview, on page 23 to drill down on the source of the problem and, if it turns out to be a service fault, restart the problem service.

If you see alarms indicating that one hybrid node has failed, or that one hybrid node and one or more worker nodes have failed, start by attempting to reboot or replace (erase and then readd) the failed nodes. If you are still having trouble after that, consider performing a clean system reboot.

The loss of two or more hybrid nodes is a double fault. Even if you replace or reboot the failed hybrid nodes, there is no guarantee that the system will recover correctly. There may also be cases where the entire system has degraded to a bad state. For such states, you can deploy a new cluster, and then recover the entire system using a recent backup taken from the old cluster.

Important

- Unintentional VM shutdown is not supported on a 3 VM cluster that is running the Crosswork Network Controller solution. If a VM fails, the remaining two VMs cannot support all the pods being migrated from the failed VM. You must deploy additional worker nodes to enable the VM shutdown.
- Reboot of one of the VMs is supported in a 3 VM cluster. In case of a reboot, the VM restore can take from 5 minutes (if the `orch pod` is not running in the rebooted VM) up to 25 minutes (if the `orch pod` is running in the rebooted VM).

The following two sections describe the steps to follow in each case.

Clean System Reboot (VMware)

Follow these steps to perform a clean system reboot:

1. Put Crosswork in Maintenance mode. See Manage Maintenance Mode Settings, on page 38 for more details.

Note (Optional) Before switching to maintenance mode, shut down the Crosswork Data Gateways and any other non-essential components (such as NSO and SR-PCE) that communicate with Crosswork.

2. Power down the VM hosting each node:
   a. Log in to the VMware vSphere Web Client.
   b. In the **Navigator** pane, right-click the VM that you want to shut down.
   c. Choose **Power** > **Power Off**.
   d. Wait for the VM status to change to **Off**.
3. Repeat Step 2 for each of the remaining VMs, until all the VMs are shut down.
4. Power up the VM hosting the first of your hybrid nodes:

a. In the **Navigator** pane, right-click the VM that you want to power up.

b. Choose **Power** > **Power Up**.

c. Wait for the VM status to change to **On**, then wait another 30 seconds before continuing.

5. Repeat Step 4 for each of the remaining hybrid nodes, staggering the reboot by 30 seconds before continuing. Then continue with each of your worker nodes, again staggering the reboot by 30 seconds.
6. The time taken for all the VMs to be powered on can vary based on the performance characteristics of your hardware. After all VMs are powered on, wait for a few minutes and login to Crosswork.
7. Move Crosswork out of Maintenance mode. See Manage Maintenance Mode Settings, on page 38 for more details.

Note If your Crosswork cluster is not in a healthy state, attempts to force maintenance mode will likely fail. Despite a successful attempt, application sync issues may still happen. In such cases, alarms will be generated indicating the list of failed services and the failure reason. If you face this scenario, you may still proceed with the "Redeploy and Restore" method mentioned below.

8. Restart the Crosswork Data Gateways and any other components in your ecosystem that communicate with Crosswork.

Redeploy and Restore (VMware)

Follow these steps to redeploy and recover your system from a backup. Note that this method assumes you have taken periodic backups of your system before it needed recovery. For information on how to take backups, see Manage Crosswork Network Controller Backup and Restore, on page 8.

1. Power down the VM hosting each node:
   a. Log in to the VMware vSphere Web Client.
   b. In the **Navigator** pane, right-click the VM that you want to shut down.
   c. Choose **Power** > **Power Off**.
   d. Wait for the VM status to change to **Off**.
   e. Repeat these steps as needed for the remaining nodes in the cluster.
2. Once all the VMs are powered down, delete them:
   a. In the VMware vSphere Web Client **Navigator** pane, right-click the VM that you want to delete.
   b. Choose **Delete from Disk**.
   c. Wait for the VM status to change to **Deleted**.
   d. Repeat these steps as needed for the remaining VM nodes in the cluster.
3. Deploy a new Cisco Crosswork cluster, as explained in *Cisco Crosswork Network Controller 6.0 Installation Guide*.

4. Recover the system state to the newly deployed cluster, as explained in Restore Crosswork Network Controller After a Disaster, on page 11.

Collect Cluster Logs and Metrics

As an administrator, you can monitor or audit the components of your Cisco Crosswork cluster by collecting periodic logs and metrics for each cluster component. These components include the cluster as a whole, individual node in the cluster, and the microservices running on each of the nodes.

Crosswork Network Controller provides logs and metrics using the following showtech options:

- **Request All** to collect both logs and metrics.
- **Request Metrics** to collect only metrics.
- **Collect Logs** to collect only logs.
- **View Showtech Jobs** to view all showtech jobs.

Note Showtech logs must be collected separately for each application.

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 To collect logs and metrics for the cluster, click **Actions** and select the showtech option that you want to perform.

Step 4 To collect logs and metrics for any node in the cluster:

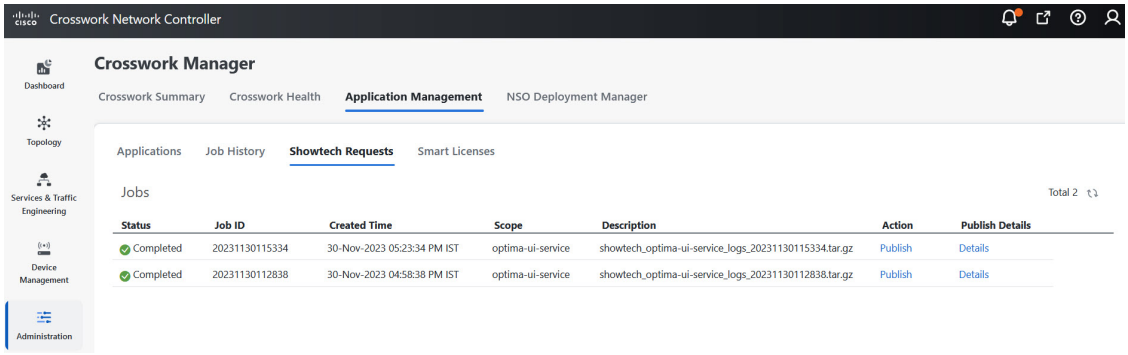
a) Click the node tile.

b) Click **Showtech Options** and select the operation that you want to perform.

Step 5 To collect logs and metrics for the individual microservices running on the VM node, click ... under the **Actions** column. Then select the showtech option that you want to perform.

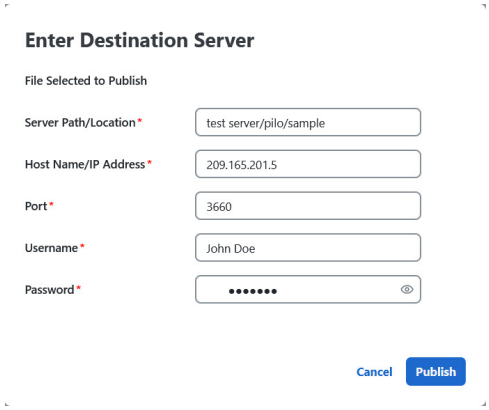
Step 6 (Optional) Click **View Showtech Jobs** to view the status of your showtech jobs. The **Showtech Requests** window displays the details of the showtech jobs.

Figure 14: Showtech Requests window

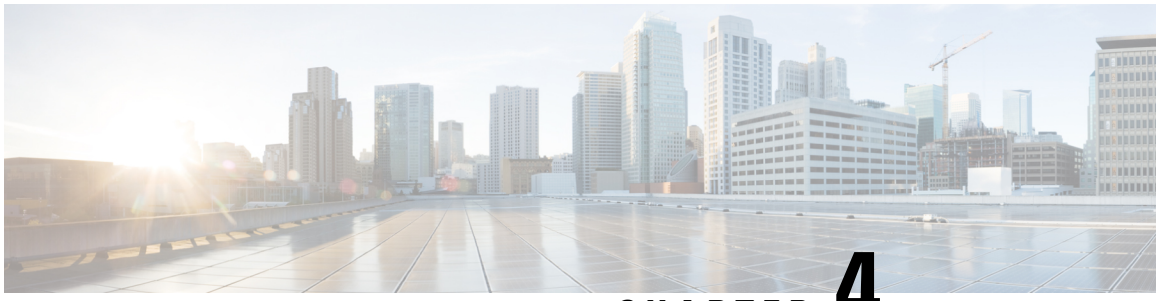


Step 7 Click **Publish** to publish the showtech logs. The **Enter Destination Server** dialog box is displayed. Enter the relevant details and click **Publish**.

Figure 15: Destination Server window



Step 8 Click **Details** to view details of the showtech log publishing.



CHAPTER 4

Cisco Crosswork Data Gateway

This section contains the following topics:

Overview of Crosswork Data Gateway

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

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

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

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

Crosswork Data Gateway uses the following concepts:

- **Crosswork Data Gateway Instance**: A Crosswork Data Gateway or a data gateway instance that you install.
- **Crosswork Data Gateway Profile**: Data gateway supports the following deployment profiles:
  - **Standard**: for use with all Crosswork applications, except Crosswork Health Insights, and Crosswork Service Health (Automated Assurance).
  - **Extended**: for use with Crosswork Health Insights and Crosswork Service Health (Automated Assurance).

Attention The **Standard with Extra Resources** profile is available as a limited-availability feature and must not be used while deploying data gateway in your data center.

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

  Operations such as attaching or detaching devices, creating collection jobs happen on the data gateway.
- **Data Destination**: Internal or external recipients of data collected by the data gateway. By default, Cisco Crosswork is defined as a data destination. Other destinations (external users) can be defined using the Cisco Crosswork UI or APIs.
- **Collection Job**: A task that data gateway has to complete to collect data. Crosswork applications create collection jobs to check device reachability, collect telemetry data needed to determine network and service health. The Cisco Crosswork UI and API allow you to configure collection jobs for non-Crosswork applications.
- **Custom Software Packages**: Files and device model definitions to extend device coverage and support data collection from currently unsupported devices.

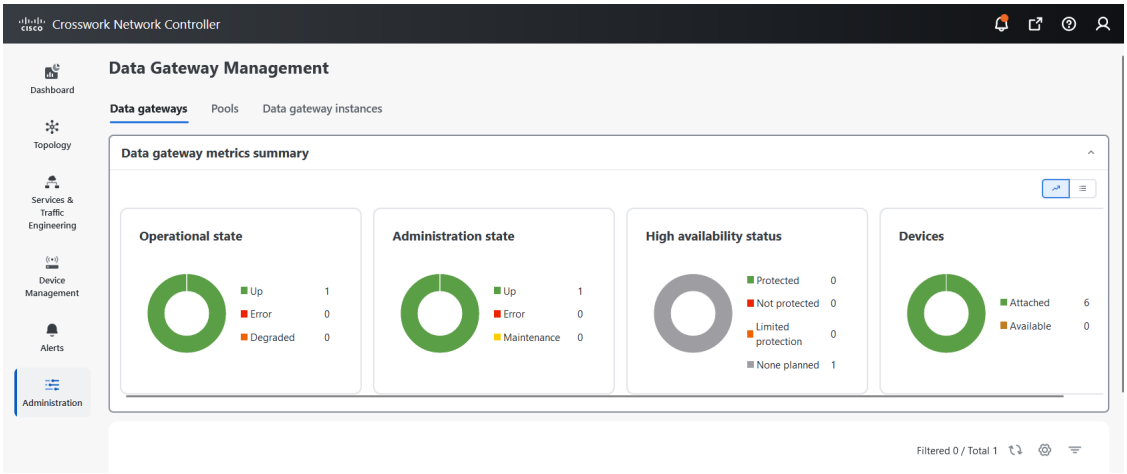
Note This chapter explains only the data gateway features that can be accessed via Cisco Crosswork UI.

For more information about the Interactive Console of the data gateway instance and how to manage it, see **Appendix A**: Configure Crosswork Data Gateway Instance, on page 391.

Crosswork Data Gateway UI Overview

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

Figure 16: Data Gateway Management Window



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

- **Data gateways**: Displays details of the virtual data gateways in the network. You can attach or detach devices to the Data Gateway from this tab.
- **Pools**: Manages the data gateway pools.
- **Data gateways instances**: Manages virtual the data gateway instances.

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

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

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

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

Table 6: Crosswork Data Gateway UI

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

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

Column	Description
Outage history	Outage history of the data gateway instance over a period of 14 days. State aggregation for a day is done in the order of precedence as Error, Degraded, Up, Unknown and Not Ready. For example, if the data gateway instance went Unknown to Degraded to Up, color is displayed as Degraded (orange) for that day as Degraded takes precedence over Up and Unknown. If the data gateway was in Error state at any time during that day, the tile is Red. If the Data Gateway was not in Error but in Degraded State anytime of the day, the tile is Orange. If the data gateway was not in Error or Degraded state and was only Up, then the tile is Green.
Average availability	Value indicating the health of the data gateway instance. This percentage is calculated as the total time (in milliseconds) a data gateway was in UP state over the time between start time of first event and end time of last event. **Note** The end time of the last event is the current time stamp, so the duration of the last event is between its start time and the current time stamp.

Column	Description
Data gateway instance name	Name of the data gateway that is created automatically when you add a data gateway instance to a pool. Clicking the icon next to the instance name displays the enrollment details of each instance. This includes details such as, the: • Instance name • Description • Instance type • Instance role • CPU • Memory • Number of NICs • Instance UUID • Instance OS version • Interface name • Interface role(s) • Interface mac • Interface name The **Additional interface role information** describes the interface roles available in data gateway.
Attached device count	Indicates the number of the devices that are attached to the data gateway pool.
PDG identifier	Unique identifier of the physical data gateway instance.
Actions	Click to view the actions that you can perform on the pool: • Attach devices. For more information, see Attach Devices to a Crosswork Data Gateway, on page 63. • Detach devices. For more information, see Manage Crosswork Data Gateway Device Assignments, on page 71. • Move devices. For more information, see Manage Crosswork Data Gateway Device Assignments, on page 71. • Initiate a failover. For more information, see Perform a Manual Failover, on page 62.

You can configure the Crosswork Data Gateway dashlet in the **Crosswork Home** page > **Dashboard**. The dashboard allows you to customize the dashlet to display the summary of the data gateway instances and pools. For information on using Dashboard, see Overview of the Topology Map, on page 201.

Set Up Crosswork Data Gateway To Collect Data

Before setting up the data gateways, it's essential to have a good understanding of how Crosswork must be setup. For more information, see Setup Workflow, on page 3.

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

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

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

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

Table 7: Tasks to Complete to Set Up Crosswork Data Gateway to Collect Data

Task	Follow the steps in...
1. Create data gateway pools.	Create a Data Gateway Pool, on page 54
2. (Optional) Create data gateway pools in the geo redundancy-enabled sites.	Create a Pool in the Geo Redundancy-Enabled Sites, on page 58
2. Attach devices to the data gateway.	Attach Devices to a Crosswork Data Gateway, on page 63
3. Verify that the default collection jobs are created and running successfully.	Monitor Collection Jobs, on page 130
4. (Optional) Extend device coverage to collect data from currently unsupported devices or third-party devices.	Device Packages, on page 84
5. (Optional) Forward data to the external data destinations.	Create and Manage External Data Destinations, on page 77
6. (Optional) Create custom collection jobs that are independent of the ones that are built by Cisco Crosswork.	Crosswork Data Gateway Collection Jobs, on page 93

Crosswork Data Gateway High Availability with Pools

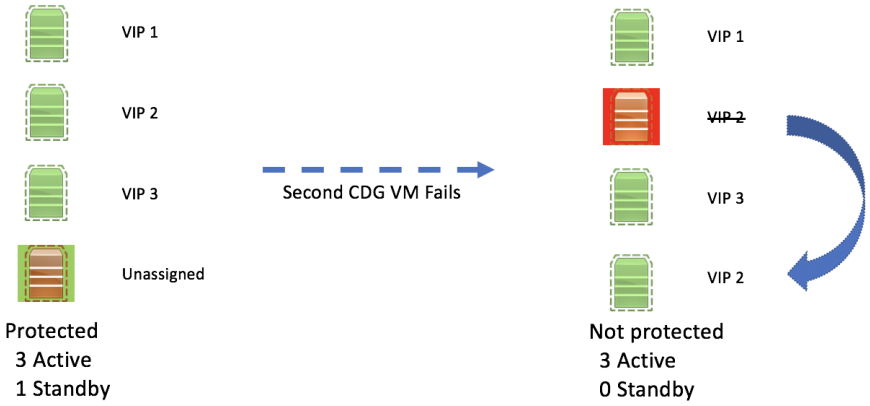
A Crosswork Data Gateway pool ensures that your device-specific data collection occurs with minimal disruption.

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

If a data gateway instance in the pool goes down, Cisco Crosswork automatically replaces that instance with a standby instance from the pool (failover) or lets you manually initiate a failover. For information on how to initiate a failover, see Perform a Manual Failover, on page 62.

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

Figure 17: Crosswork Data Gateway High Availability



Note If more than one data gateway instance in a pool has the same Southbound IP address, reboot the standby data gateway, so that the standby data gateway instance loses its southbound IP address when it comes up.

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

A Crosswork Data Gateway pool has the following states:

- **Protected**: All instances are UP and there is at least one standby instance in the pool.
- **Not protected**: All the standby instances are DOWN and there are none available to replace an instance that is in use.
- **Limited protection**: Some standby instances are DOWN, but there is still at least one standby that is UP.

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

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

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

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

Create a Data Gateway Pool

Before you begin

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

- Certain fields and configuration options are only accessible with the geo redundancy feature enabled. For information about the geo redundancy capabilities, see the *Enable Geo Redundancy* section in *Cisco Crosswork Network Controller 7.0 Installation Guide*.
- **Enable FQDN for secure syslog communication** data gateway supports secure syslog communication to devices which require the syslog certificate to contain the hostname or FQDN instead of the virtual IP address of the data gateway. This is an optional feature that can be enabled for devices which mandate having the hostname or FQDN in the syslog certificate. If enabled, Cisco Crosswork fetches the hostname or FQDN for each virtual IP address of the data gateway from the DNS server. FQDNs for newly added virtual IP(s) will be fetched after you save the pool. The syslog certificate will then contain the FQDN in the CN and SAN instead of the virtual IP address of the data gateway. For details on how to configure secure syslog on devices, see Configure Secure Syslog on Device, on page 111.
- Have network information such as virtual IP address (one virtual IP for each active data gateway), subnet mask and gateway information ready.

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

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

- An additional IP address on the Data Network for 2 NIC deployment.
- An IP address on the Southbound Network for 3 NIC deployment.

- Decide if you wish to enable FQDN for virtual IP(s) addresses in the pool. If yes, ensure that you have configured FQDN for virtual IP(s) in the DNS server to create the pool successfully.
- Make sure you have installed a minimum of one data gateway or, if you prefer high availability, at least two data gateways. The number of data gateways is determined by your network requirements. If you need assistance, contact the Cisco Customer Experience team.

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

Pool UI terminologies

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

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

Pool creation guidelines

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

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

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

Step 2 In the **Pools** tab, click the + button and select one of the following:

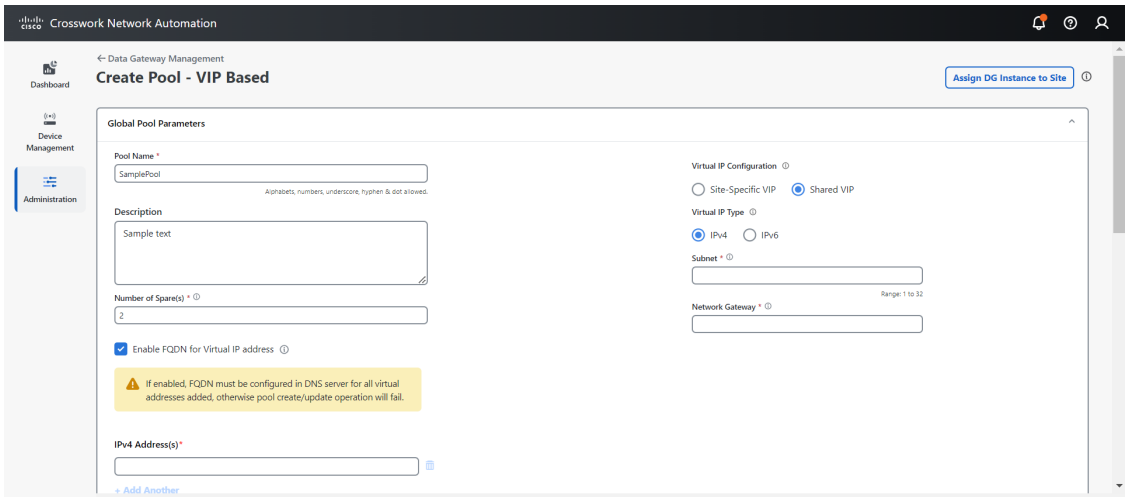
- **VIP-based**
- **FQDN-based**

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

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

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

Figure 18: VIP-based Pool Creation Window for Single Stack Deployment



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

Figure 19: VIP-based Pool Creation Window for Dual-Stack Deployment

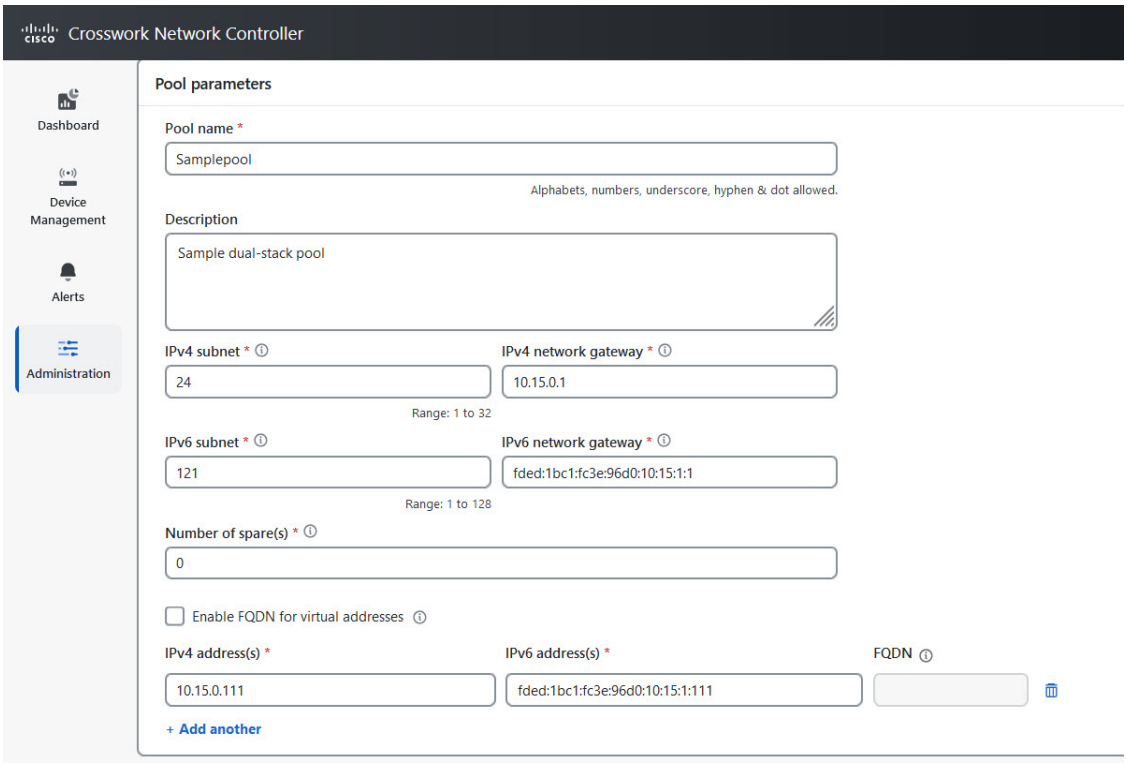
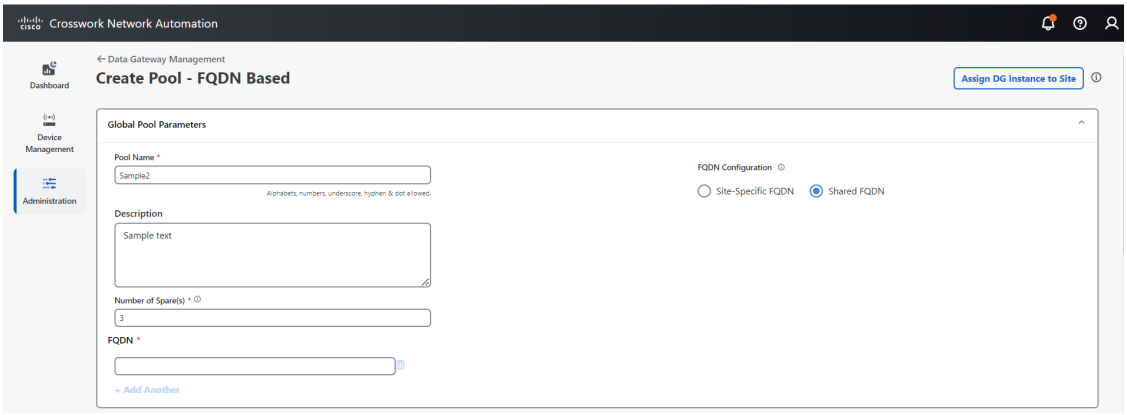


Figure 20: FQDN-based Pool Creation Window



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

If you are creating a pool in the geo redundancy-enabled deployment, from here on follow the procedure in Create a Pool in the Geo Redundancy-Enabled Sites, on page 58. For non-geo deployment, continue with the steps in this document.

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

Step 6 Click **Create**.

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

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

Create a Pool in the Geo Redundancy-Enabled Sites

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

The following procedure describes how to configure the additional fields.

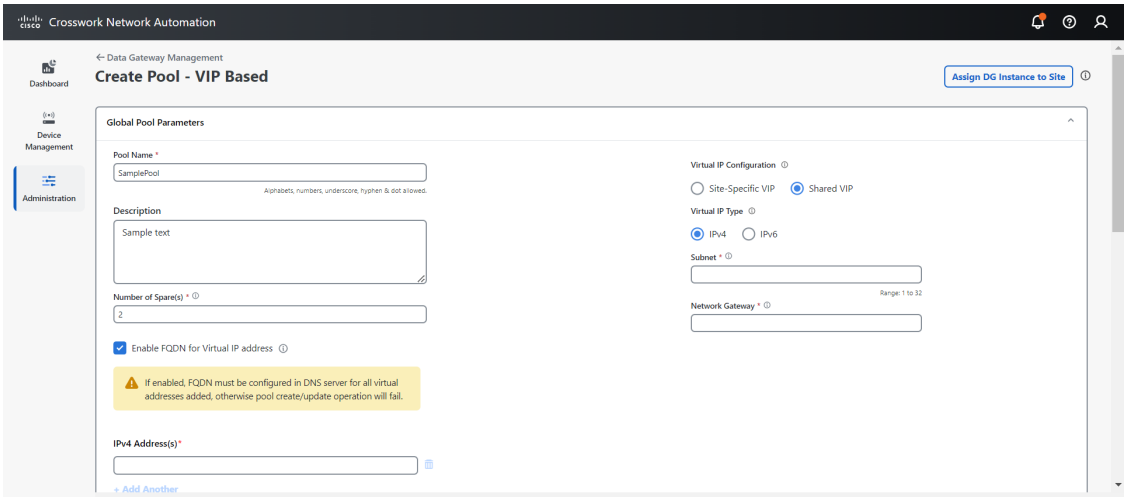
Before you begin

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

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

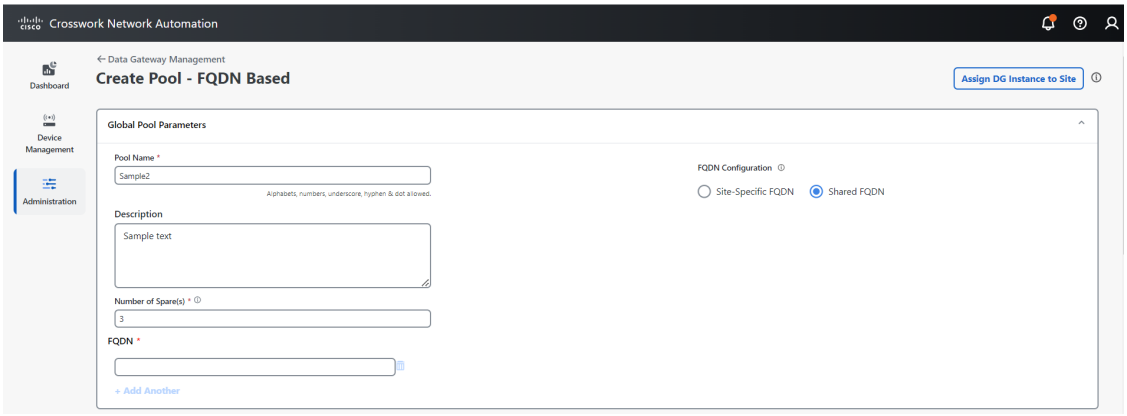
- **VIP-based pool**:
  - Under **Virtual IP configuration**, select **Shared VIP** or **Site-specific VIP**.
  - If you have selected **Shared VIP**, enter the following:
    - **Virtual IP type**: Select either an IPv4 or IPv6 address family for virtual IPs.
    - For dual stack deployment, specify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

Figure 21: VIP-Based Pool Creation Window



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

Figure 22: FQDN-based Pool Creation Window



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

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

Figure 23: Active Pane for Single Stack

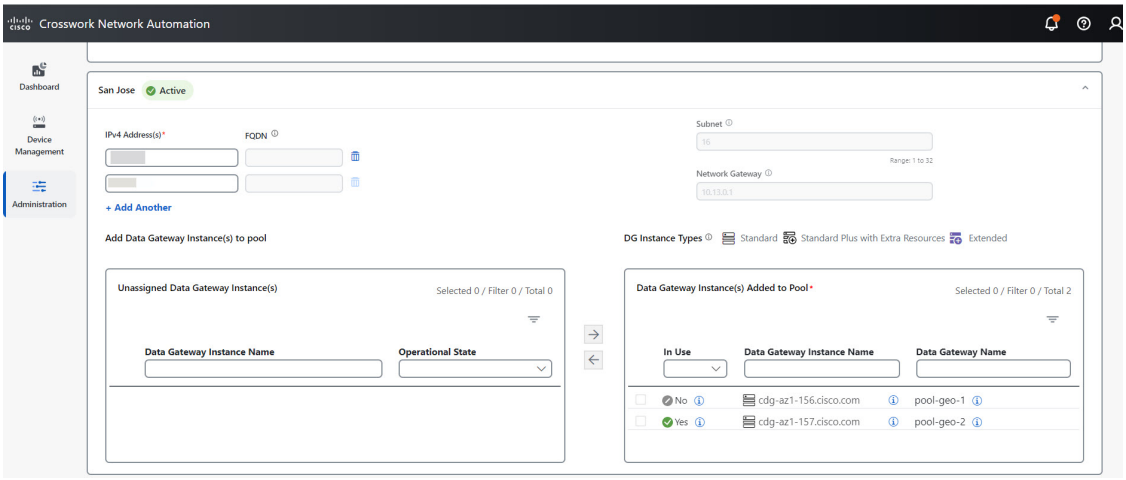
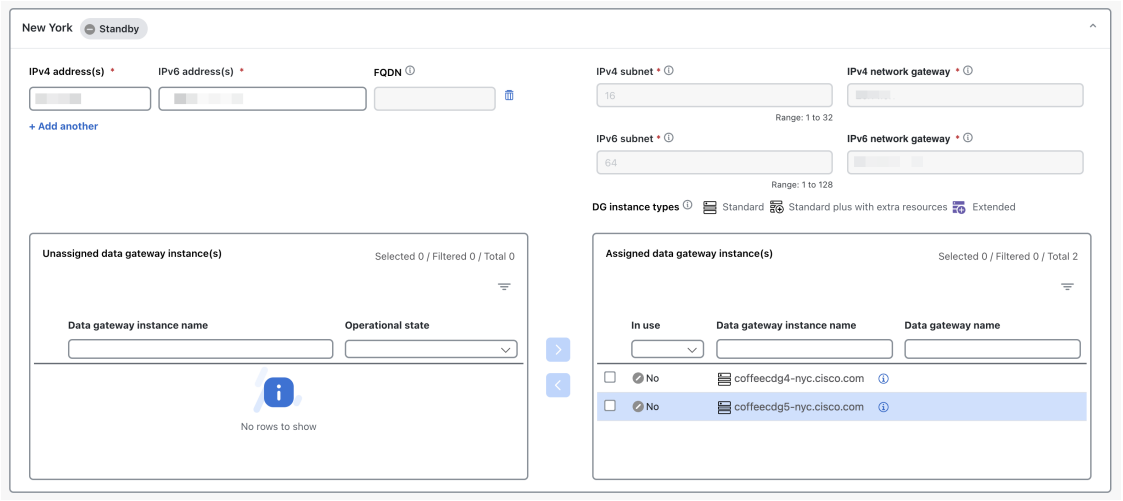


Figure 24: Active Pane for Dual Stack



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

Figure 25: Standby Pane for Single Stack

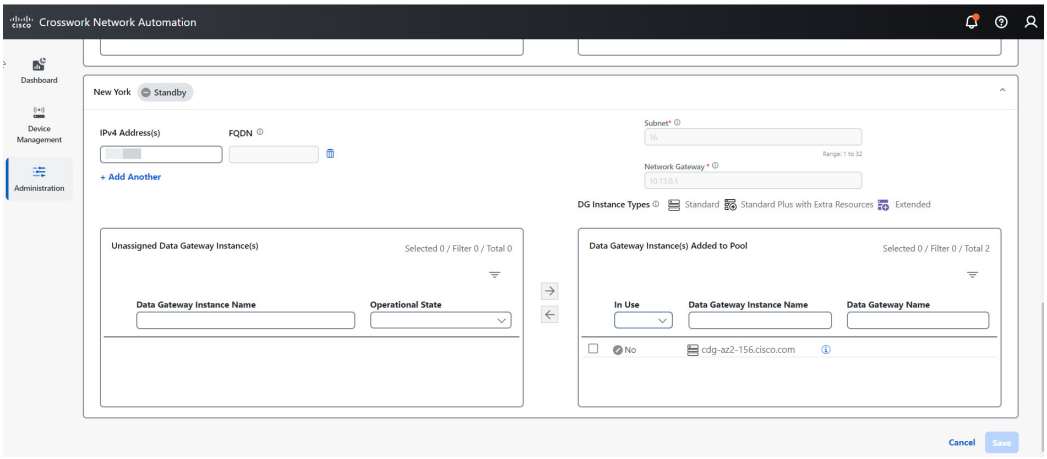
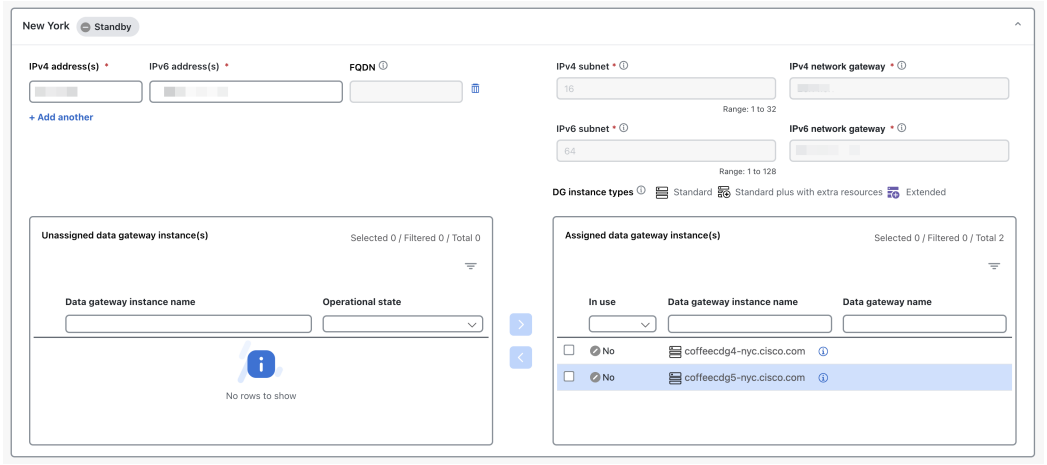


Figure 26: Standby Pane for Dual Stack



Step 5 Click **Create**.

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

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

Assign Data Gateways to Geo Redundancy-Enabled Sites

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

Before you begin

Ensure that you are aware of the following:

- The data gateway instances can be assigned to sites only with the Geo Redundancy feature is enabled. For information on how to enable the Geo Redundancy capabilities, see the *Enable Geo Redundancy* section in *Cisco Crosswork Network Controller 7.0 Installation Guide*.
- When the data gateways are in the unassigned state, you have the option to assign them to either an Active or Standby site.
- If the data gateway is a member of a pool, you can assign it to a site only during Crosswork migration using the edit pool option. During the Crosswork migration, a notification is shown on the **Data Gateway Management** page, to indicate the ongoing migration.

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

Step 2 Click **Assign DG instance to site**. The **Assign data gateway instance(s) to site** window opens. The window displays the data gateway instances in the unassigned state.

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

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

Step 5 Click **Assign**.

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

Perform a Manual Failover

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

Before you begin

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

- Manual failover cannot be attempted on a data gateway for which the autofailover is in-progress.
- Crosswork allows only one failover request at a time. It does not support multiple failover requests at the same time.
- Confirm that at least one instance has the operational state as **NOT_READY**. Crosswork considers this instance as the standby on which the failover happens.
- At least one spare data gateway should be present in both the standby and active cluster, with the status of **NOT_READY**.
- A data gateway in the maintenance mode cannot be used as a spare for the future failover procedures until the administration state as **UP**.

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

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

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

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

Step 4 Click **Continue**.

What to do next

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

If the failover is unsuccessful due to an error, see Data Gateway Failover Failed, on page 141.

Attach Devices to a Crosswork Data Gateway

Before you begin

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

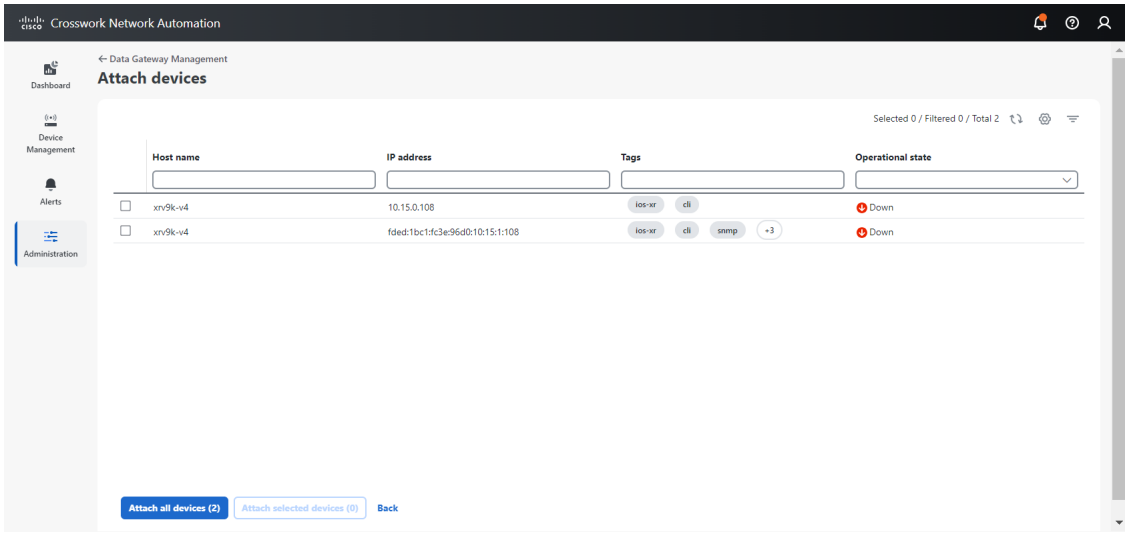
- 3des-cbc
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-96
- hmac-sha1
- hmac-md5-96
- hmac-md5
- hmac-sha2-256-etm@openssh.com
- hmac-sha2-512-etm@openssh.com

Step 1 (Optional) Before attaching devices to an existing Crosswork Data Gateway, we recommend that you check the health of the Crosswork Data Gateway. See Monitor Crosswork Data Gateway Health, on page 65 for more information.

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

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

Figure 27: Attach Devices Window



Step 4 To attach all the devices, click **Attach all devices**. Otherwise, select the devices you want to attach and click **Attach selected devices**.

Step 5 In the **Confirm - Attach devices** dialog, click **Attach**.

Verify that your changes are successful by checking the **Attached device count** column in the **Data gateways** pane.

Monitor the Crosswork Data Gateway health to ensure that the Crosswork Data Gateway is functioning well with the newly attached devices. For information on how to monitor the heath, see Monitor Crosswork Data Gateway Health, on page 65.

Manage Crosswork Data Gateway Post-Setup

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

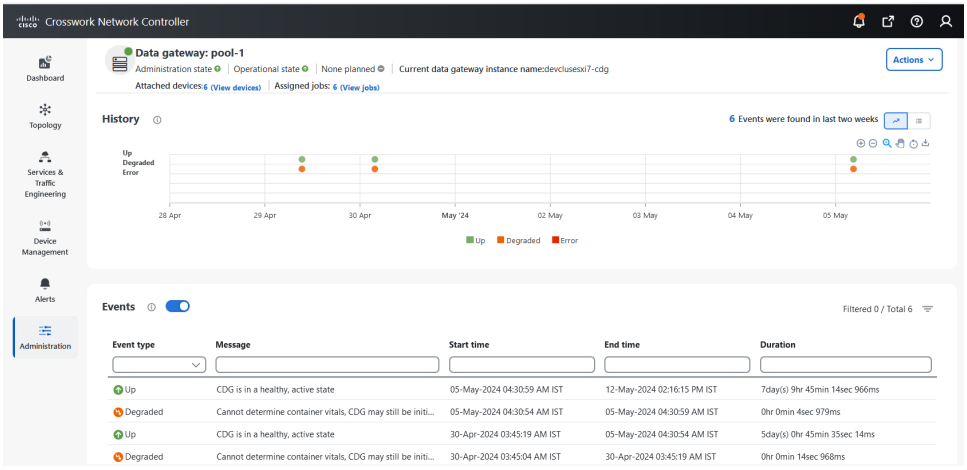
Monitor Crosswork Data Gateway Health

You can view the operations and health summary of a data gateway from the Crosswork Data Gateway vitals page. To access this page, go to **Administration > Data Gateway Management > Data gateways** and click the pool name in the table. The pool details page opens. This page also has details of the health of various containerized services running on a data gateway. The overall health of a data gateway depends on the health of each containerized service.

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

- **Ping**–Checks the reachability to any IP address.
- **Trace route**–Helps troubleshoot latency issues. This option provides you with a time estimate for the data gateway to reach the destination.
- **Download service metrics**–Downloads the metrics for all collection jobs for a data gateway from the Cisco Crosswork UI.
- **Download showtech**–Downloads the showtech logs from Cisco Crosswork UI.
- **Reboot**–Reboots the data gateway.
- **Change log level**–Allows you to change the log level of a data gateway's components, for example collectors (cli-collector) and infra services (oam-manager). Log level changes apply only to the data gateway on which you are making the change.

Figure 28: Data Gateway Window



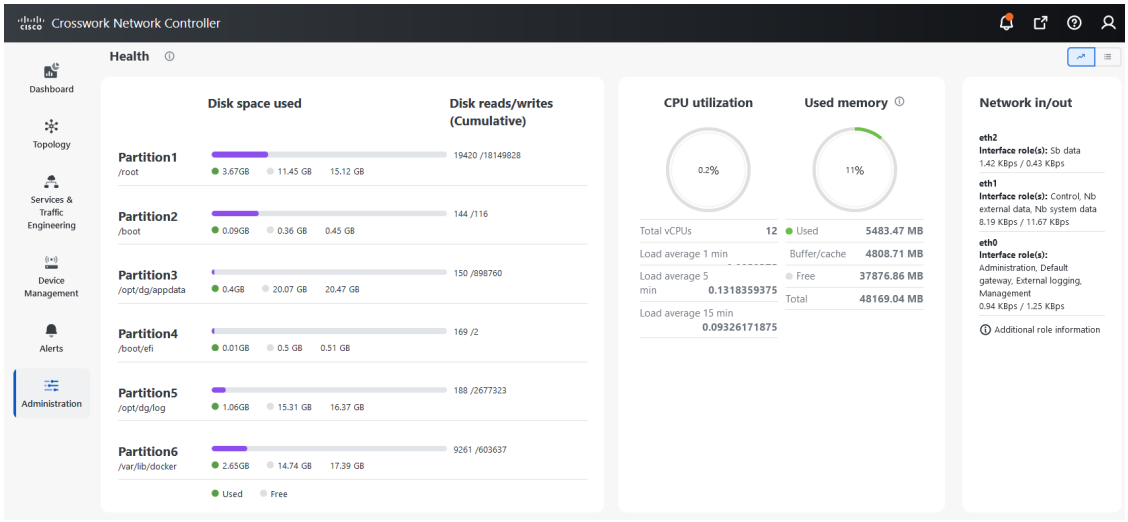
The following parameters are displayed on this page:

- **General Crosswork Data Gateway details**–Displays general details of data gateway including operational state, high availability state, attached device count, and assigned jobs. The **Actions** option lists the various troubleshooting options that are available from the UI.
- **History**–Shows the outage history chart of data gateway over 14 days including timestamp, outage time, and clear time. Use the options in the top-right corner of the pane to zoom in, zoom out, pan, or download the SVG and PNG of the history chart of a specific time period within the graph.
- **Events**–Displays a list of all the data gateway transition state changes over the last 14 days. It includes information such as the event details, including operational state changes, role changes, a message indicating the reason for the status change, timestamp, and duration.
- **Health**–Shows the health information of the data gateways. The timestamp in the top-right corner is the timestamp when the last health data was collected. If the data gateway is in an **Error** state or if the data is stale for any reason, the timestamp label highlights that the data is old. If the **CPU utilization** of a data gateway exceeds 80%, we recommend taking corrective action before the **CPU utilization** increases further leading to failure of the data gateway.

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

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

Figure 29: Crosswork Data Gateway Health Window

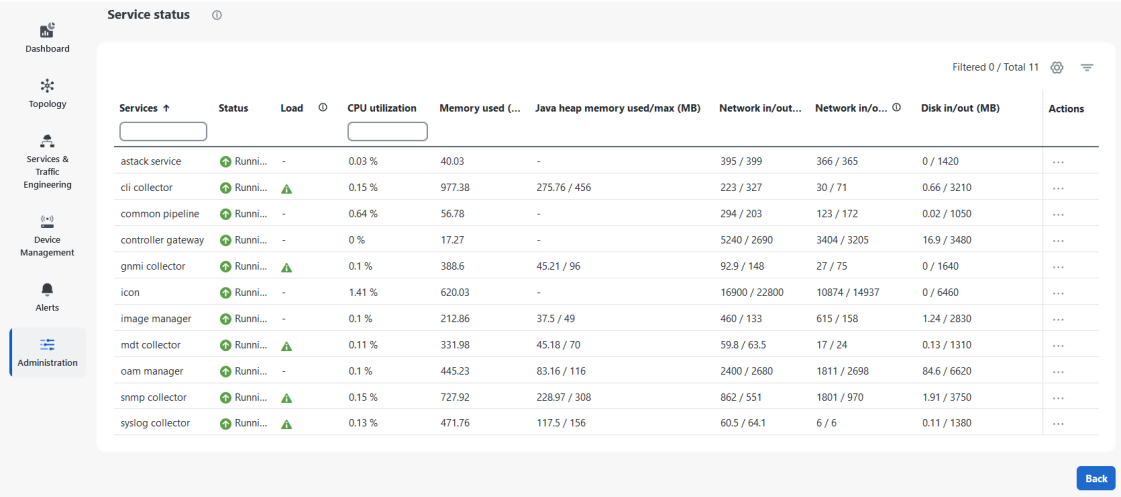


- **Service status**–Displays the health information of the individual container services running on the data gateway and their resource consumption with an option to restart (**Actions > Restart**) an individual service. The Load column indicates the processing load of that specific collector/service.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

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

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

Figure 30: Service Status Window



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

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

   The alarms include the event title, severity, the configuration stage (Day 0, 1, or 2), description, and the remediation action. For more information on how to navigate to the **Showtech Requests** window, see Viewing Crosswork Data Gateway Alarms, on page 68.

2. If the **CPU utilization** of a data gateway exceeds 80%, we recommend that you do not create more collection jobs until you have reduced the **CPU utilization** by moving devices to another data gateway, have added other VMs to the pool, or increase the cadence of existing collection jobs.

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

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

Viewing Crosswork Data Gateway Alarms

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

To view the alarms, navigate to the Crosswork UI:

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

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

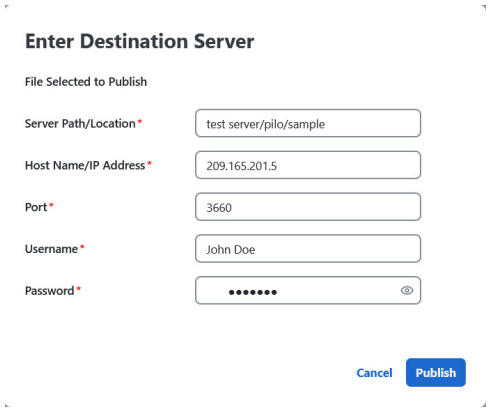
Step 2 In the **Platform Infrastructure** tile, click **View Details**. The **Application Details** window opens.

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

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

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

Figure 31: Showtech Requests Window



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

Edit or Delete a Crosswork Data Gateway Pool

Follow the steps to edit or delete a data gateway pool. To create a pool, see Create a Data Gateway Pool, on page 54 or Create a Pool in the Geo Redundancy-Enabled Sites, on page 58.

Before you begin

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

- Virtual data gateways or pools that have devices that are attached cannot be deleted.
- A date gateway instance can be removed from the pool only when all the mapped devices are unmapped from Crosswork Data Gateway. When a data gateway instance is removed from the pool, a standby instance from the same pool becomes its replacement after you perform a failover procedure. For information about manual failovers, see Perform a Manual Failover, on page 62.
- Before you delete a data gateway pool, detach devices from the data gateway first or move the devices to another data gateway.

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

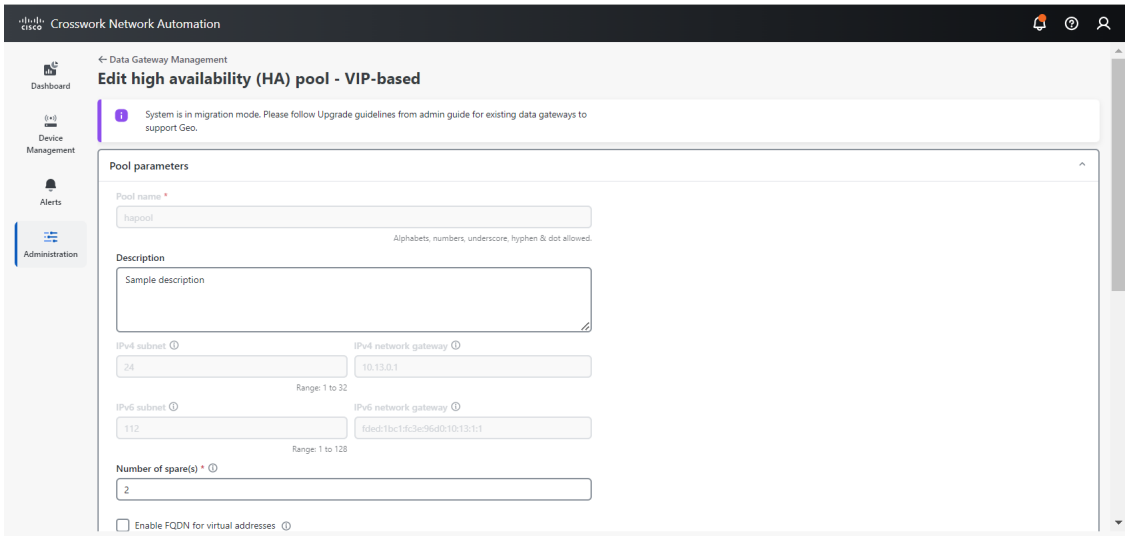
Step 2 **Edit high availability (HA) pool**:

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

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

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

Figure 32: Data Gateway Management - Edit HA Pool Window



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

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

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

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

Step 3 **Delete a data gateway pool**:

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

b) Click **Delete** in the **Delete high availability (HA) pool** window to delete the pool.

Manage Crosswork Data Gateway Device Assignments

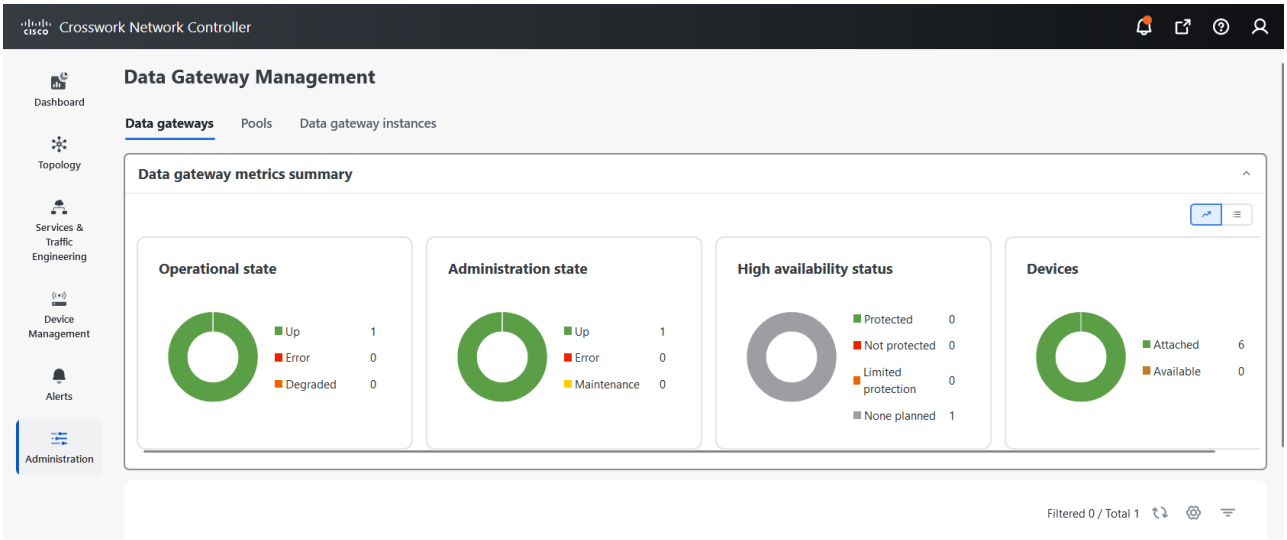
Follow these guidelines when you move or detach devices from a Crosswork Data Gateway.

- A device can be attached to only one Crosswork Data Gateway.
- When moving devices to a Crosswork Data Gateway in a different pool, ensure that the Gateway of the pool is same as the Gateway of the current pool. Moving devices to a Crosswork Data Gateway with mismatching gateway results in failed collections.
- Detaching a device from Crosswork Data Gateway deletes all collection jobs corresponding to the device. If you do not want to lose the collection jobs submitted for the device you wish to detach, move the device to another data gateway instead.

Follow the steps below to move or detach devices from a Crosswork Data Gateway pool. To add devices to the pool, see Attach Devices to a Crosswork Data Gateway, on page 63.

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

Figure 33: Data Gateways Window

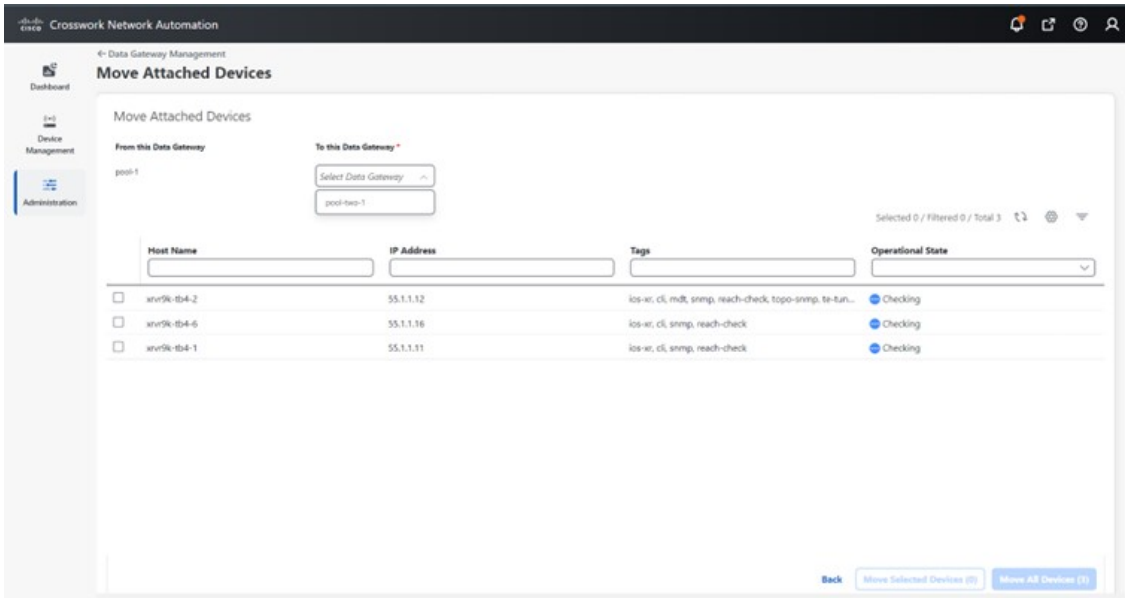


Step 2 **Move Devices**:

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

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

Figure 34: Move Attached Devices Window



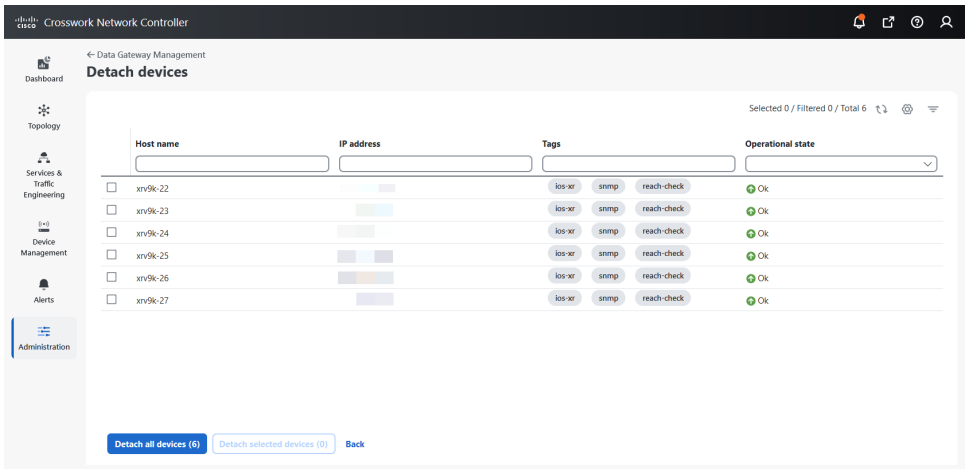
c) To move all the devices, click **Move all devices**. Otherwise, select the devices you want to move and click **Move selected devices**.

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

Step 3 **Detach Devices**:

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

Figure 35: Detach Devices Window



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

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

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

For information on how initiate a failover, see Perform a Manual Failover, on page 62.

Maintain Crosswork Data Gateway Instances

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

- Change the Administration State of Crosswork Data Gateway Instance, on page 73
- Delete Crosswork Data Gateway Instance from Crosswork Network Controller, on page 74
- Redeploy a Crosswork Data Gateway Instance, on page 76

Change the Administration State of Crosswork Data Gateway Instance

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

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

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

Note In the **Assigned** state, a data gateway cannot be switched directly to the maintenance mode. To enter the maintenance mode, you must either execute a manual failover when standby is available or remove the data gateway from the pool. See Perform a Manual Failover, on page 62 for information on manual failover.

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

Before you begin

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

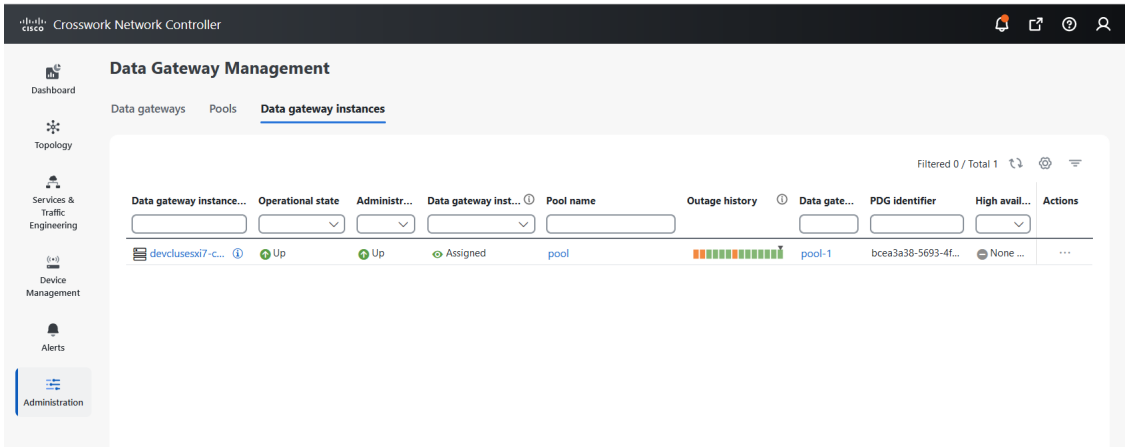
- Spare role when a manual or autofailover occurs.
- Assigned role when it is the only gateway in the pool.

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

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

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

Figure 36: Data Gateway Instances Window



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

Delete Crosswork Data Gateway Instance from Crosswork Network Controller

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

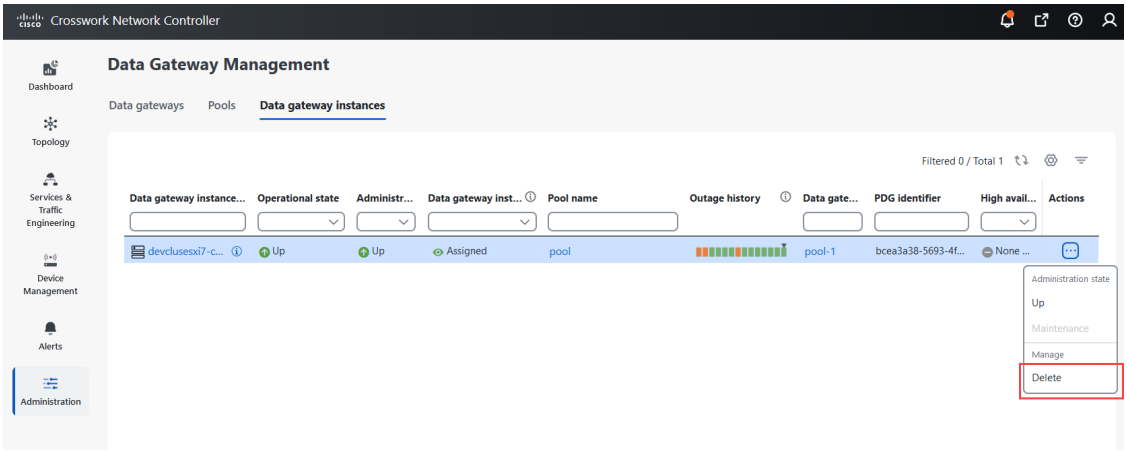
Before you begin

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

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

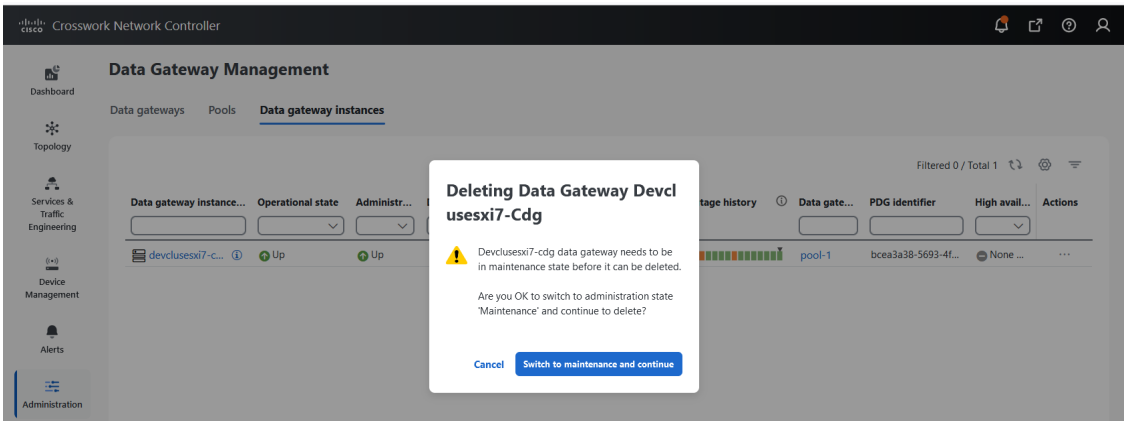
Step 2 For the Crosswork Data Gateway that you want to delete, click ··· under the **Actions** column and click **Delete**.

Figure 37: Data Gateway Instances Window



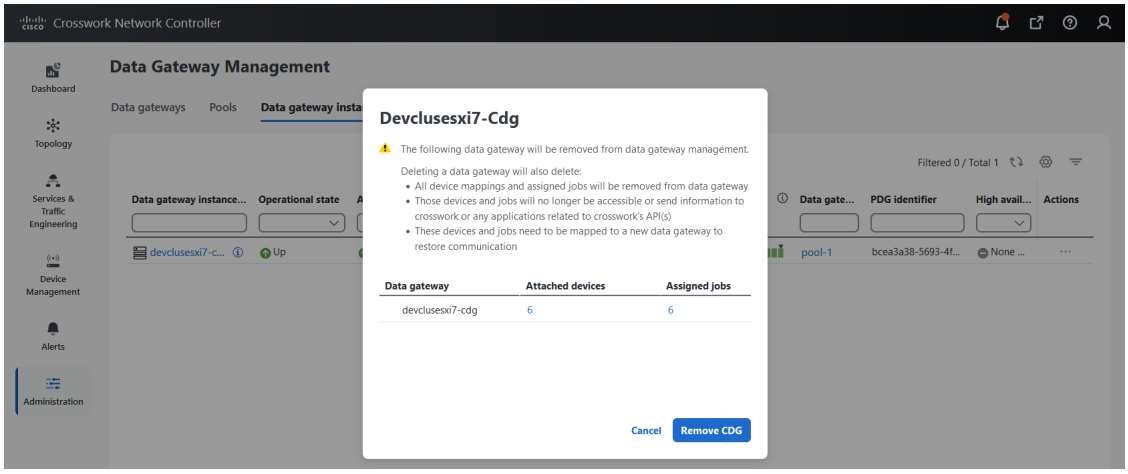
Step 3 The Crosswork Data Gateway instance must be in maintenance mode to be deleted. Click **Switch to maintenance & continue** when prompted to switch to **Maintenance** mode.

Figure 38: Switch to Maintenance & Continue Pop-up Window



Step 4 Check the check box for **I understand the concern associated with deleting the Data Gateways** and click **Remove CDG**.

Figure 39: Delete Data Gateway Confirmation Dialog Box



Redeploy a Crosswork Data Gateway Instance

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

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

Important points to consider

- If the data gateway instance was already enrolled with Cisco Crosswork and you have installed the instance again with the same name, change the **Administration state** of the data gateway instance to **Maintenance** for auto-enrollment to go through.
- If a data gateway instance was already enrolled with Cisco Crosswork and Cisco Crosswork was installed again, re-enroll the existing data gateway instance with Cisco Crosswork. See Re-enroll Crosswork Data Gateway, on page 418.
- If you are redeploying a data gateway instance with the same hostname, clear the existing alarms for that hostname to avoid confusion. Otherwise, the old alarms will still be viewable in the history. With the old alarms, you must check the timestamps. This is necessary to determine whether they were raised on the older data gateway or the current one with the same hostname.

Configure Crosswork Data Gateway Global Settings

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

- Device Packages, on page 84
- Configure Crosswork Data Gateway Global Parameters, on page 88
- Allocate Crosswork Data Gateway Resources, on page 90

Create and Manage External Data Destinations

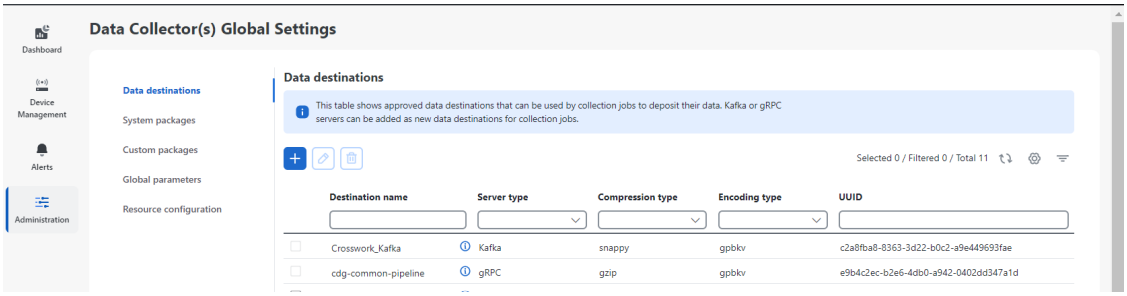
Cisco Crosswork allows you to create external data destinations (Kafka or external gRPC) that can be used by collection jobs to deposit data.

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

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

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

Figure 40: Data Destinations Window



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

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

Licensing Requirements for External Collection Jobs

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

1. From the main menu, go to **Administration** > **Application Management** > **Smart License**.
2. Select **Crosswork Platform Services** in the application field.
3. Ensure that the status is as follows:
   - **Registration Status - Registered**

     Indicates that you have registered with Cisco Smart Software Manager (CSSM) and are authorized to use the reserved licensed features.
   - **License Authorization Status - Authorized** (In Compliance).

     Indicates that you have not exceeded the device count in the external collection jobs.

- Under Smart Licensing Usage, **CW_EXTERNAL_COLLECT** has status as **In Compliance**.

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

Add or Edit a Data Destination

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

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

- If you reinstall an already existing external Kafka data destination with the same IP address, then the collectors need to be restarted for changes to take effect.
- You can secure the communication channel between Cisco Crosswork and the specified data destination that is, either Crosswork Kafka or external Kafka. (See **Step 6** in this procedure). However, enabling security can impact performance.
- If your external data destination requires a TLS connection, keep the public certificate ready or if it requires client authentication, keep the client certificate and key files ready. The client key might be password-encrypted which needs to be configured as part of the data destination provisioning. Currently, Crosswork Data Gateway supports IP-based certificates only.
- Ensure that the certificates are PEM encoded and the key file is in PKCS#8 format when generating them with your Certificate Authority.
- Ensure that you create the Kafka topics before you submit the job in Cisco Crosswork. Depending on the external Kafka and how topics are managed in that external Kafka, Cisco Crosswork logs may show the following exception if the topic does not exist at the time of dispatching the collected data to that specific external Kafka / topic. This could be because the topic is not created yet or the topic was deleted before the collection job was complete.

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

- Check and validate the port connectivity for the data destination. If the port is unreachable in the destination, it leads to a failed collection.
- Crosswork Data Gateway allows you to configure custom values in the destination properties for a Kafka destination (see Step 4 in this procedure).

Note This feature is not supported on a gRPC destination.

- Global properties entered in the **Destination Details** pane are mandatory and will be applied to the Kafka destination by default unless there are custom values specified at the individual collector level. Custom values that you specify for a collector apply only to that collector.
- The external destination must be IPv4 or IPv6 depending on the protocol specified when deploying Crosswork Data Gateway. For instance, if IPv4 was chosen during the deployment, the external destination should also be IPv4.

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

Before you begin

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

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

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

- `num.io.threads = 8`
- `num.network.threads = 3`
- `message.max.bytes= 30000000`

- You have created Kafka topics that you want to be used for data collection.
- Ensure that 'reachability-topic' is configured on the Kafka destination before a new collection job is started. This configuration is required for monitoring the health of the Kafka destination.

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

Step 2 In the **Data destinations** page, click + button. The **Add destination** page opens.

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

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

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

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

Field	Value	Available in gRPC	Available in Kafka
Encoding type	From the drop-down, select the encoding (json or gpbkv).	Yes	Yes
Compression type	From the drop-down, select the compression type.	Yes Supported compression types are Snappy, gzip, lz4, zstd, and none. **Note** zstd compression type is supported only for Kafka 2.0 or higher.	Yes Supported compression types are Snappy, gzip, and deflate.
Dispatch Type	This field is available when the **Server Type** field is set to **gRPC**. From the drop-down, select the dispatch method as stream or unary. Crosswork Data Gateway transmits the collected data to the destination as data streams or unary. The default value is unary.	Yes	No
Maximum message size (bytes)	Enter the maximum message size in bytes. • **Default value**: 100000000 bytes/ 30 MB • **Min**: 1000000 bytes/1 MB • **Max**: 100000000 bytes/ 30 MB	No	Yes
Buffer memory	Enter the required buffer memory in bytes. • **Default value**: 52428800 bytes • **Min**: 52428800 bytes • **Max**: 314572800 bytes	No	Yes
Batch size (bytes)	Enter the required batch size in bytes. • **Default value**: 6400000 bytes/6.4 MB • **Min**: 16384 bytes/ 16.38 KB • **Max**: 6400000 bytes/6.4 MB	No	Yes

Field	Value	Available in gRPC	Available in Kafka
Linger (milliseconds)	Enter the required linger time in milliseconds. • **Default value**: 5000 ms • **Min**: 0 ms • **Max**: 5000 ms	No	Yes
Request timeout	Enter the duration that the request waits for a response. After the configured duration is met, the request expires. • **Default value**: 30 ms • **Min**: 30 ms • **Max**: 60 ms	Yes	Yes

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

Step 4 (Optional) To configure custom values that are different from global properties for a Kafka destination, in the **Destination - Per collector properties** pane:

a) Select a **Collector**.

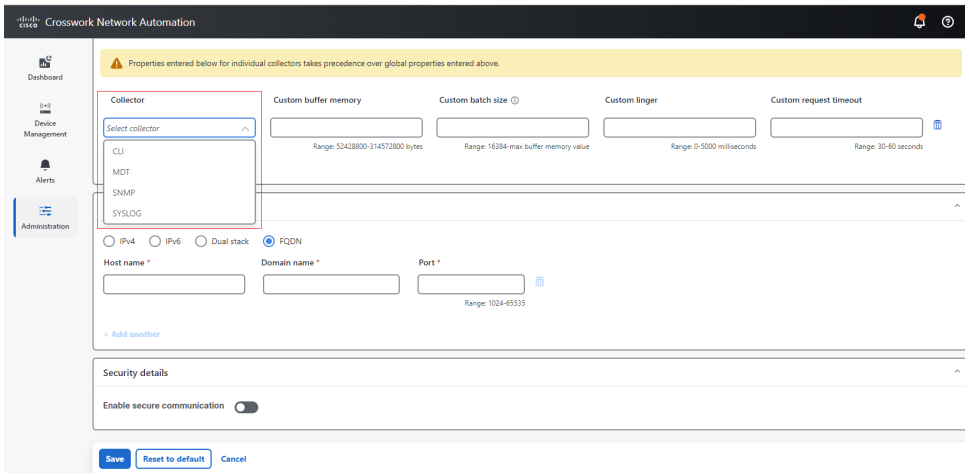
b) Enter values for the following fields:

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

  Note The **Custom batch size** cannot exceed the value of the **Custom buffer memory** at run time. In case, you do not provide a value in the **Custom buffer memory** field, the **Custom batch size** will be validated against the value in the **Buffer memory** field.

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

Figure 41: Add Destination Window



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

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

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

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

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

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

Connectivity Type	Fields	Available in gRPC	Available in Kafka
IPv4	Enter the required **IPv4 address/ Subnet mask**, and **Port**. You can add multiple IPv4 addresses by clicking **+ Add another** IPv4 subnet mask ranges from 1 to 32 and port range from 1024 to 65535.	Yes	Yes
IPv6	Enter the required **IPv6 address/ Subnet mask**, and **Port**. You can add multiple IPv6 addresses by clicking **+ Add another**. IPv4 subnet mask ranges from 1 to 32 and port range from 1024 to 65535. IPv6 subnet mask ranges from 1 to 128 and port range from 1024 to 65535.	Yes	Yes

Connectivity Type	Fields	Available in gRPC	Available in Kafka
Dual Stack	Enter the **IPv4 address/ Subnet mask**, **IPv6 address/ Subnet mask**, and **Port**. You can add multiple addresses by clicking **+ Add another**.	Yes	Yes
FQDN	Enter the required **Host name**, **Domain name**, and **Port**. The supported port range is from 1024 to 65535. You can add multiple FQDN addresses by clicking **+ Add nnother**.	Yes	Yes

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

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

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

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

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

Step 9 Click **Save**.

What to do next

If you have enabled the **Enable secure communication** option, navigate to the **Certificate Management** page in the Cisco Crosswork UI (**Administration > Certificate Management**) and add the relevant certificate for the newly added data destination. This step is mandatory to establish a secure communication to the device. See Manage Certificates, on page 289 for more information.

Note If you do not add the certificate or the certificate is incomplete for the data destination after enabling the **Enable secure communication** option, Cisco Crosswork sets the destination to an error state. When the destination is in an error state, the collection job status will be degraded.

Delete a Data Destination

Follow the steps to delete a data destination:

Before you begin

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

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

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

Step 3 In **Delete data destination(s)** pop up, click **Delete** to confirm.

Device Packages

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

The system device and MIB packages are bundled in the Crosswork software and are automatically downloaded to the system instances. You cannot modify the system device and MIB packages. Custom device package extends device coverage and collection capabilities to third-party devices. Suppose the default package that Crosswork provides does not suit your environment, such as if you need to collect data from a third-party device or want specific data that the default MIB package does not support. In that case, customize the package and upload it to Crosswork. For assistance with the customization of the package, contact Cisco or your Cisco partner.

Custom Packages

You can upload the following types of custom packages to Cisco Crosswork:

1. **CLI device package**: To use CLI-based KPIs to monitor device health for third-party devices. All custom CLI device packages along with their corresponding YANG models should be included in file `custom-cli-device-packages.tar.xz`. Multiple files are not supported. However, you can use the aggregate package if you want to bundle different files for different devices in a single package.
2. **Custom MIB package**: Custom MIBs and device packages can be specific to third-party devices or be used to filter the collected data or format it differently for Cisco devices. These packages can be edited. All custom SNMP MIB packages along with YANG models should be included in file `custom-mib-packages.tar.xz`. Multiple files are not supported.

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

3. **SNMP device package**: Crosswork Data Gateway allows you to extend the SNMP coverage by uploading custom SNMP device packages with any additional MIB and YANG descriptions you require.
4. **Aggregate package**: The aggregate package option allows you to include multiple supported file extensions in a single package. These files can be collector and application-specific files. For instance, an aggregate package can consist of files for CLI and SNMP device packages.

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

   Collector files:

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

Application files:

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

Workflow for Adding a Custom Package

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

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

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

Add Custom Packages

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

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

Note Crosswork Network Controller does not validate the files being uploaded other than checking the file extension.

Follow these steps to upload a custom software package:

Before you begin

- When uploading new MIBs as a part of the Custom MIB Package, ensure that those new MIBs files can be uploaded within collectors along with the existing System MIB files that are, all dependencies in the files are resolved properly.
- If you plan on adding an Aggregate package, ensure that:
  - The package must contain only supported file extensions. For a list of supported extensions, refer to Custom Packages, on page 84.
  - The files must only be bundled in the .tar.gz format.
  - The top-level directory must contain at least one of the specified collector types:
    - snmp
    - cli
    - common

Sample directory structure:

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

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

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

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

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

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

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

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

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

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

Step 6 Click **Upload**.

What to do next

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

Delete Custom Package

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

Follow the steps to delete a custom package:

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

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

Step 3 In the **Delete custom package** window that appears, click **Delete** to confirm.

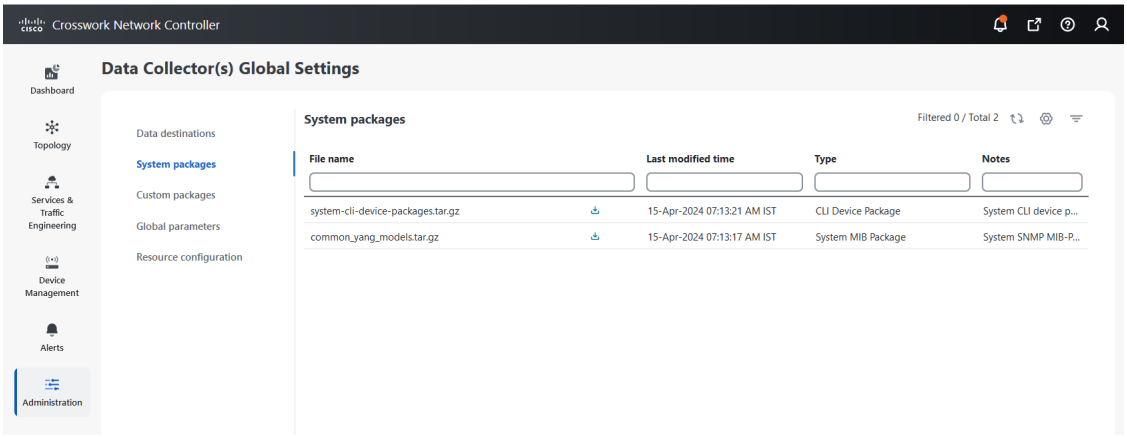
System Device Package

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

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

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

Figure 42: System Device Packages Window



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

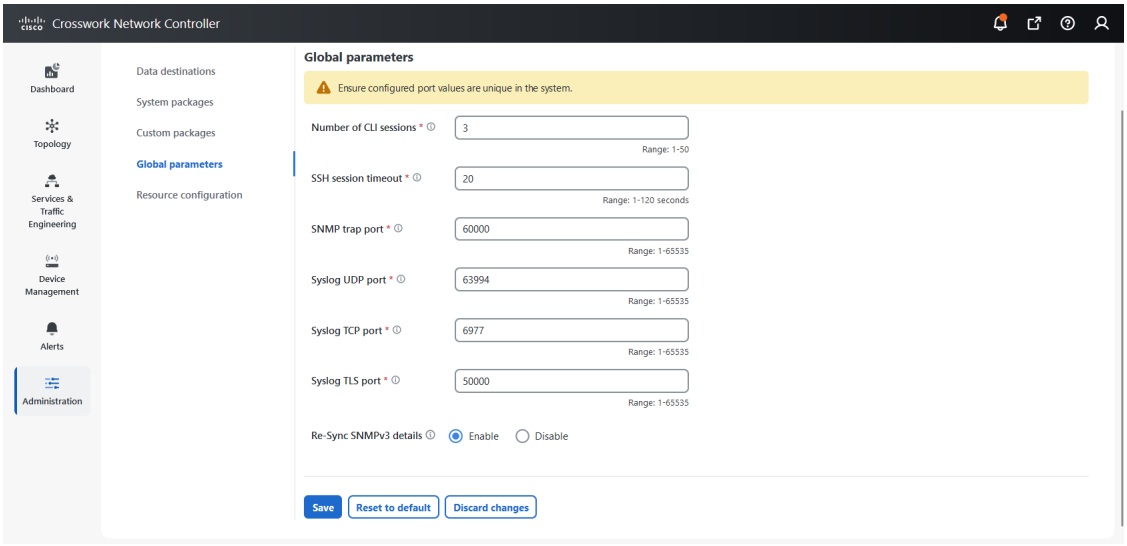
Configure Crosswork Data Gateway Global Parameters

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

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

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

Figure 43: Global Parameters Window



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

To properly update port values, you should:

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

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

Parameter Name	Description	Default value for cluster VM deployment
Syslog TLS port	-	6514 Accepted range is 1–65535
Re-Sync SNMPv3 details	USM details change whenever a device is rebooted or reimaged. SNMPV3 collections stop working whenever there is a change in any of the USM details. Enable this option to sync the USM details automatically whenever there is a change, after the first collection failure.	Disable

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

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

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

1. If all the Crosswork Data Gateways were updated successfully, a success message appears in the UI indicating that the update was successful.
2. If any of the Crosswork Data Gateways in the network could not be updated, an Error window appears in the UI. Crosswork Data Gateway will automatically try to update the parameters on the failed Crosswork Data Gateway during recovery. Some of the collectors might be restarted as part of the recovery.

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

What to do next

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

Allocate Crosswork Data Gateway Resources

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

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

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

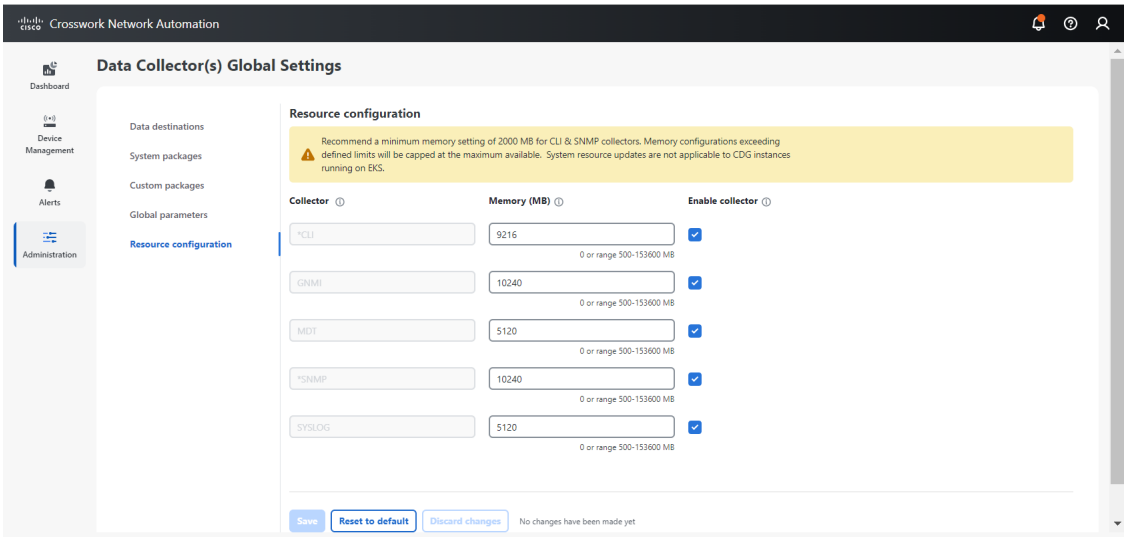
Note The list of collectors that is displayed on this page is dynamic, that is, it is specific to the deployment.

To update resource allocation for collectors:

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

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

Figure 44: Resource Configuration Window



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

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

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

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

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

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

Enable or Disable Collectors

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

To enable or disable the collectors:

Before you begin

Review the following information before enabling or disabling a collector:

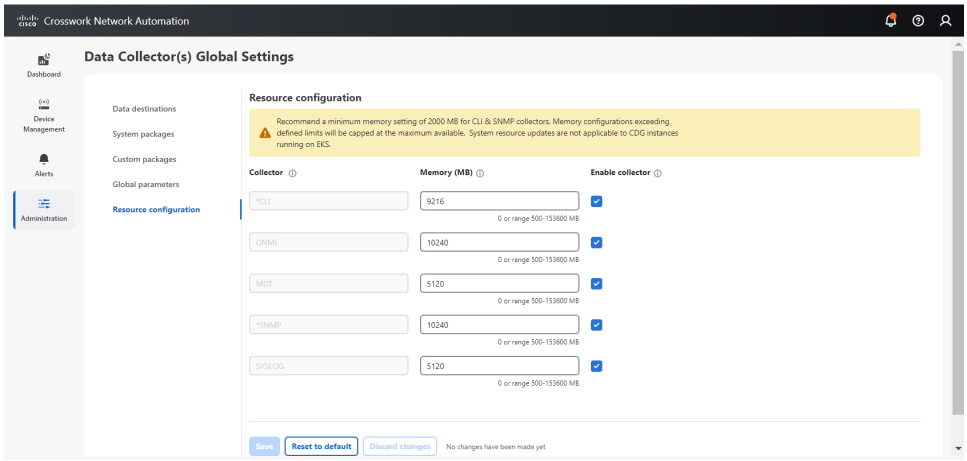
- The data collection for the SNMP and CLI collectors (containers) cannot be disabled. These collectors are required to check the device reachability.
- By default, the collectors are in the enabled state.

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

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

The list of collectors and the resource limits is displayed.

Figure 45: Enabling or Disabling Collectors



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

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

Step 3 Click **Save** to apply your changes.

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

Crosswork Data Gateway Collection Jobs

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

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

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

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

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

1. Data collection request to forward data for internal processes within Crosswork. Cisco Crosswork creates system jobs for this purpose. If you want the data gateway to collect specific information from non-Cisco devices, you must use custom device packages. For more information on custom device packages, see Custom Packages, on page 84.

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

2. Data collection request to forward data to external data destinations. For more information on configuring the external data destinations (Kafka or gRPC), see Create and Manage External Data Destinations, on page 77.

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

Note Crosswork Data Gateway drops incoming traffic if there is no corresponding (listening) collection job request for the same. It also drops data, syslog events, and SNMP traps received from an unsolicited device (that is, not attached to Crosswork Data Gateway).

You can view collection jobs currently active on all the data gateway instances enrolled with Crosswork Network Controller from the **Collection Jobs** page.

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

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

For more information, see Monitor Collection Jobs, on page 130.

Types of Collection Jobs

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

- CLI Collection Job, on page 94
- SNMP Collection Job, on page 95
- MDT Collection Job, on page 103
- Syslog Collection Job, on page 105
- gNMI Collection Job, on page 114

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

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

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

The **Cadence** value determines the frequency at which data gateway collects the data from the device. You can set the frequency between 10 and 604800000 milliseconds. We recommend a cadence of minimum 60 milliseconds.

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

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

CLI Collection Job

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

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

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

You can create a CLI collection job from the Cisco Crosswork UI or using APIs. For information on creating a job from the UI, see Create a Collection Job from Cisco Crosswork UI, on page 125 and from the API, see Cisco DevNet.

Sample Payload of CLI Collection API

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

1. The device is identified with a UUID rather than an IP address.
2. The destination is also referenced by a UUID. For collections jobs built using the UI, Cisco Crosswork looks up the UUIDs. When you create your own collection jobs, you must look up these values.

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

SNMP Collection Job

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

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

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

After the OIDs are resolved, they are provided as input to the SNMP collectors. You can create the SNMP OID-based collection jobs from the Cisco Crosswork UI or using the API, and SNMP-traps using the API.

The device packages can be imported into the Crosswork Data Gateway instance as described in Section Add Custom Packages, on page 85.

Supported SNMP versions for data polling and traps are:

- Polling Data
  - SNMPv2
  - SNMPv3 (no auth nopriv, auth no priv, authpriv)
  - Supported auth protocols – SHA-1, MD5
  - Supported priv protocols – AES-128, AES-192, AES-256, CiscoAES192, CiscoAES256, DES, and 3-DES.
- Traps
  - SNMPv2
  - SNMPv3 (no auth nopriv, auth no priv, authpriv)

Sample Configurations on Device:

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

Table 8: Sample configuration to enable SNMP on device

Version	Command	To...
V2c	`snmp-server group <group_name> v2c` `snmp-server user <user_name> <group_name> v2c`	Define the SNMP version, user/user group details.
	`snmp-server host <host_ip> traps SNMP version <community_string> udp-port 1062` `snmp-server host a.b.c.d traps version 2c v2test udp-port 1062`	Define the destination to which trap data must be forwarded. **Note** The IP address mentioned here must be the virtual IP address of the Crosswork Data Gateway.
	`snmp-server traps snmp linkup` `snmp-server traps snmp linkdown`	Enable traps to notify link status.

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

The SNMP Collector supports the following operations:

- SCALAR

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

- TABLE
- WALK
- COLUMN

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

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

The value for snmpRequestTimeoutMillis should be specified in milliseconds:

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

Following is an SNMP collection job sample:

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

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

SNMP Traps Collection Job

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

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

Crosswork Data Gateway listens on UDP port 1062 for Traps.

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

SNMP Trap Collection Job Workflow

On receiving an SNMP trap, Crosswork Data Gateway:

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

Note To prevent Crosswork Data Gateway from checking the community string for SNMP traps, select the **SNMP Disable Trap Check** check box when adding a device through the Crosswork UI. For more information about this option, see Add Devices Through the User Interface, on page 282.

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

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

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

If the collection job is invalid, there is missing configuration on the device, or no trap is received, the status of the job remains "Unknown". For list of supported Traps and MIBs, see List of Pre-loaded Traps and MIBs for SNMP Collection, on page 421.

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

Table 9: List of Supported Non-Yang/OID based Traps

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

Following is an SNMP-Trap collection job sample:

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

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

Enabling Traps forwarding to external applications

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

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

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

- Link up

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4
  ```

- Link Down

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3
  ```

- Syslog

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.9.9.41.2.0.1
  ```

- Cold Start

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1
  ```

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

```
      "snmpTrap": {
        "version": "V2c",
        "pduType": "TRAP",
        "v2v3Data": {
          "agentAddress": "172.70.39.227",
          "oidRecords": [
            {
              "oid": "1.3.6.1.2.1.1.3.0",
              "strValue": "7 days, 2:15:17.02"
            },
            {
              "oid": "1.3.6.1.6.3.1.1.4.1.0",  // This oid is the Object Identifier.
              "strValue": "1.3.6.1.6.3.1.1.5.3" // This is the value that determines the
kind of trap.
            },
            {
              "oid": "1.3.6.1.2.1.2.2.1.1.8",
              "strValue": "8"
            },
            {
              "oid": "1.3.6.1.2.1.2.2.1.2.8",
              "strValue": "GigabitEthernet0/0/0/2"
            },
            {
              "oid": "1.3.6.1.2.1.2.2.1.3.8",
              "strValue": "6"
            },
            {
              "oid": "1.3.6.1.4.1.9.9.276.1.1.2.1.3.8",
              "strValue": "down"
            }
          ]
        }
      }
    }
  ],
  "collectionEndTime": "1580931985267",
  "collectorUuid": "YmNjZjEzMTktZjFlOS00NTE5LWI4OTgtY2Y1ZmQxZDFjNWExOlRSQVBfQ09MTEVDVE9S",
  "status": {
    "status": "SUCCESS"
  },
  "modelData": {},
  "sensorData": {
    "trapSensor": {
      "path": "1.3.6.1.6.3.1.1.5.4"
    }
  },
  "applicationContexts": [
    {
      "applicationId": "APP1",
      "contextId": "collection-job-snmp-traps"
    }
  ]
}
```


MDT Collection Job

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

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

- MDT TCP Dial-out Mode

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

Note

- If there is some change (update) in existing MDT jobs between backup and restore operations, Crosswork Network Controller does not replay the jobs for config update on the devices as this involves NSO. You have to restore configs on NSO/devices. Crosswork Network Controller only restores the jobs in database.
- Before using any YANG modules, check if they are supported. See Section: List of Pre-loaded YANG Modules for MDT Collection , on page 429

Following is a sample of MDT collection payload:

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

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

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

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

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

MDT Collection Job Workflow

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

1. Sends a configuration request to NSO to enable the data collection on the target devices.
2. Send a collection job create request to the Crosswork Data Gateway.
3. Crosswork Data Gateway creates a distribution to send the data collected to the destination you specify.

Syslog Collection Job

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

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

The following syslog formats are supported:

- RFC5424 syslog format
- RFC3164 syslog format

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

While the order of the configuration steps does not matter, you must complete both the steps, or no data are sent. For sample device configuration, see Configure Non-secure Syslog on Device, on page 109. Cisco Crosswork also allows you to set up secure syslog communication to the device. For more information, see Configure Secure Syslog on Device, on page 111.

Sample syslog collection payload

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

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

- You can filter the output of syslog data collection by specifying either PRI-based SyslogSensor OR Filters-based SyslogSensor. The syslog events matching the facilities and severities mentioned in the payload are sent to the specified destination. All other nonmatching syslog events are dropped. You can specify the filter based on regEx, severity, or facility.
- If you have specified values for severity and facility, then both the conditions are combined based on the logical operator specified at Filters level.
- You can specify a maximum of three filters combinations using the logical operator AND or OR. By default, the AND operator is applied if do not specify an operator.

Syslog Collection Job Output

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

syslog events received from the device should be parsed by the syslog collector. You can choose either **UNKNOWN**, **RFC5424** or **RFC3164**.

Following is the sample output for each of the options:

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

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

Sample output:

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

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

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

RFC5424

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

Sample output:

```
....
....


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

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

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

RFC3164

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

Sample output:

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

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

Configure Non-secure Syslog on Device

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

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

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

Note The syslog format that you configure for the device must match the format that you specified when the device was added through the Crosswork UI. See Add Devices Through the User Interface, on page 282 for more information.

Configure RFC3164 Syslog format

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

For IOS XR:

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

For IOS XE:

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

Configure RFC5424 Syslog format

For IOS XR:

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

For IOS XE:

```
no logging message-counter syslog
logging trap <serverity>
logging facility <facility>
logging host <CDG IP> transport tcp port 9898 session-id string <sessionidstring> --> To
use TCP channel
OR
logging host <CDG IP> transport udp port 9514 session-id string <sessionidstring> ---> To
use UDP channel
OR
```

```
logging host <CDG IP> vrf Mgmt-intf transport udp port 9514 session-id string
<sessionidstring> --> To use UDP via vrf
service timestamps log datetime msec year show-timezone
logging trap syslog-format 5424 --> if applicable
```

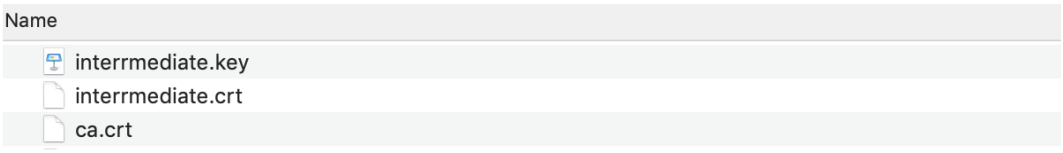
Configure Secure Syslog on Device

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

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

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

      The following files are downloaded to your system.



2. Configure the device with the Cisco Crosswork trustchain.

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

   Sample IOS XR device configuration to enable TLS

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


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

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

Read 1583 bytes as CA certificate
  Serial Number  : A7:F2:53:CF:72:8E:6A:D7:54:34:4A:05:6B:92:18:F8
  Subject:
```

```
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
                CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:09 UTC Sat Jan 16 2021
  Validity End   : 02:37:09 UTC Thu Jan 15 2026
  SHA1 Fingerprint:
                209B3815271C22ADF78CB906F6A32DD9D97BBDBA

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


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

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

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

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


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


Trustpoint       : syslog-inter
==================================================
CA certificate
```

```
  Serial Number  : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
  Subject:
        CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
        CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:11 UTC Sat Jan 16 2021
  Validity End   : 02:37:11 UTC Mon Jan 16 2023
  SHA1 Fingerprint:
         B06F2BFDE95413A8D08A01EE3511BC3D42F01E59
RP/0/RSP0/CPU0:ASR9k(config)#logging tls-server syslog-tb131
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#tls-hostname 10.13.0.159
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#severity debugging
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#vrf default
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#commit
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#exit
RP/0/RSP0/CPU0:ASR9k(config)#exit
RP/0/RSP0/CPU0:ASR9k#exit
RP/0/RSP0/CPU0:ASR9k#show running-config logging
Fri Jan 22 11:17:19.385 GMT
logging tls-server syslog-tb131
vrf default
severity debugging
trustpoint syslog-inter
tls-hostname <CDG VIP FQDN name>
!
logging trap debugging
logging format rfc5424
logging facility user
logging hostnameprefix ASR9k
logging suppress duplicates

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

Sample IOS XE device configuration to enable TLS

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

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

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

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

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


csr8kv(config)#crypto pki trustpoint syslog-intermediate
```

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

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

-----BEGIN CERTIFICATE-----
MIIFfTCCA2WgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVT
.............................................................
.............................................................
Nmz6NQynD7bxdQa9Xq9kyPuY3ZVKXkf312IRH0MEy2yFX/tAen9JqOeZ1g8canmw
TxsWA5TLzy1RmxqQh88f0CM=
-----END CERTIFICATE-----
Trustpoint 'syslog-intermediate' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
       Fingerprint MD5: FE27BDBE 9265208A 681670AC F59A2BF1
      Fingerprint SHA1: 03F513BD 4BEB689F A4F4E001 57EC210E 88C7BD19

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

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

Syslog configuration to support FQDN

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

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

For IOS XR:

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

For IOS XE:

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

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

For IOS XR:

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

For IOS XE:

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

gNMI Collection Job

Crosswork Network Controller supports gRPC Network Management Interface (gNMI) based telemetry data collection via Crosswork Data Gateway. It supports only gNMI Dial-In (gRPC Dial-In) streaming telemetry

data based on subscription and relaying subsequent subscription response (notifications) to the requested destinations.

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

To configure gNMI on the device, see Device Configuration for gNMI, on page 122.

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

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

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

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

Table 10: gNMI Subscription Options

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

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

Note

- Crosswork Data Gateway relies on the device to declare the support of one or more modes.
- gNMI sensor path with default values does not appear in the payload. This is a known protobuf behavior.

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

  Example 1:

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

  Example 2:

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

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

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

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

Enable Secure gNMI communication between Device and Crosswork Data Gateway

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

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

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

1. Generate the certificates. See Generate Device Certificates, on page 118.

2. Upload the certificates to the Crosswork Certificate Management UI in Cisco Crosswork. See Configure gNMI Certificate, on page 119.
3. Update device configuration with secure gNMI port details from Cisco Crosswork UI. See Update Protocol on Device from Cisco Crosswork, on page 122.
4. Enable gNMI on the device. See Device Configuration for gNMI, on page 122.
5. Enable gNMI bundling on the device. See Configuring gNMI Bundling for IOS XR, on page 124.
6. Configure the certificates and device key on the device. See Import and Install Certificates on Devices, on page 120.

Generate Device Certificates

This section explains how to create certificates with OpenSSL.

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

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

1. **Create the rootCA certificate**

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

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

2. **Create device key and certificate**

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

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

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

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

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

The following is a sample output:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            66:38:0c:59:36:59:da:8c:5f:82:3b:b8:a7:47:8f:b6:17:1f:6a:0f
        Signature Algorithm: sha256WithRSAEncryption
```

```
    Issuer: CN = rootCA
    Validity
        Not Before: Oct 28 17:44:28 2021 GMT
        Not After : Aug 17 17:44:28 2024 GMT
    Subject: CN = Crosswork
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:
                00:c6:25:8a:e8:37:7f:8d:1a:7f:fa:e2:d6:10:0d:
                b8:e6:2b:b0:b0:7e:ab:c9:f9:14:a3:4f:2e:e6:30:
                97:f4:cd:d6:11:7d:c0:a6:9b:43:83:3e:26:0f:73:
                42:89:3c:d7:62:7b:04:af:0b:16:67:4c:8e:60:05:
                cc:dd:99:37:3f:a4:17:ed:ff:28:21:20:50:6f:d9:
                be:23:78:07:dc:1e:31:5e:5f:ca:54:27:e0:64:80:
                03:33:f1:cd:09:52:07:6f:13:81:1b:e1:77:e2:08:
                9f:b4:c5:97:a3:71:e8:c4:c8:60:18:fc:f3:be:5f:
                d5:37:c6:05:6e:9e:1f:65:5b:67:46:a6:d3:94:1f:
                38:36:54:be:23:28:cc:7b:a1:86:ae:bd:0d:19:1e:
                77:b7:bd:db:5a:43:1f:8b:06:4e:cd:89:88:e6:45:
                0e:e3:17:b3:0d:ba:c8:25:9f:fc:40:08:87:32:26:
                69:62:c9:57:72:8a:c2:a1:37:3f:9d:37:e9:69:33:
                a5:68:0f:8f:f4:31:a8:bc:34:93:a3:81:b9:38:87:
                2a:87:a3:4c:e0:d6:aa:ad:a7:5c:fb:98:a2:71:15:
                68:e7:8d:0f:71:9a:a1:ca:10:81:f8:f6:85:86:c1:
                06:cc:a2:47:16:89:ee:d1:90:c9:51:e1:0d:a3:2f:
                9f:0b
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Alternative Name:
            IP Address:10.58.56.18
Signature Algorithm: sha256WithRSAEncryption
     01:41:2c:91:0b:a1:10:8a:11:1a:95:36:99:2c:27:31:d3:7d:
     e9:4b:29:56:c3:b7:00:8c:f4:39:d2:8c:50:a4:da:d4:96:93:
     eb:bb:71:e3:70:d3:fe:1f:97:b2:bc:5c:f8:f4:65:ed:83:f7:
     67:56:db:0f:67:c2:3d:0c:e7:f8:37:65:1d:11:09:9a:e3:42:
     bc:c6:a0:31:7c:1f:d7:5e:c6:86:72:43:a8:c1:0c:70:33:60:
     dc:14:5b:9d:f3:ab:3d:d5:d2:94:90:1c:ba:fd:80:4d:22:e3:
     31:93:c7:16:5f:85:20:38:ad:36:b9:1a:e0:89:8e:06:8c:f8:
     cd:55:cc:a1:89:d3:91:7f:66:61:a3:40:71:c2:1e:ee:3b:80:
     37:af:73:5e:8e:0d:db:4b:49:da:a6:bd:7d:0a:aa:9e:9a:9e:
     fa:ed:05:25:08:f2:4d:cd:2f:63:55:cf:be:b1:5d:03:c2:b3:
     32:bf:f4:7b:1a:10:b9:5e:69:ac:77:5e:4a:4f:85:e3:7f:fe:
     04:df:ce:3e:bb:28:8f:e3:bf:1a:f9:0f:94:18:08:86:7d:59:
     57:71:0a:97:0d:86:9c:63:e7:0e:48:7d:f0:0e:1d:67:ff:9b:
     1d:1b:05:25:c8:c3:1f:f4:52:0f:e1:bf:86:d7:ec:47:10:bd:
     94:cf:ca:e2
```

Configure gNMI Certificate

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

Note You can upload only one gNMI certificate to Crosswork.

To add the gNMI certificate.

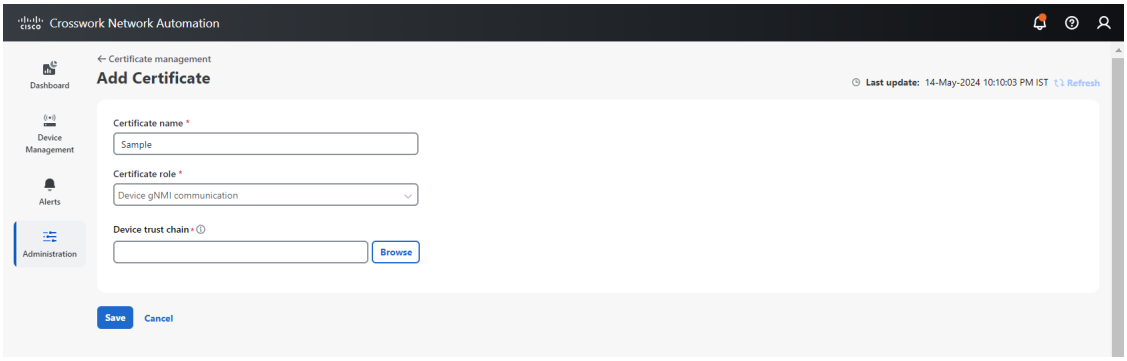
Step 1 From the Cisco Crosswork UI, go to **Administration > Certificate Management**.

Step 2 Click the + icon to add the certificate.

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

- **Certificate name** - Enter a name for the certificate.
- **Certificate role** - Select **Device gNMI Communication** from the drop-down list.
- **Device trust chain** - Browse your local file system to the location of the rootCA file and upload it.

Figure 46: Add Certificate Window

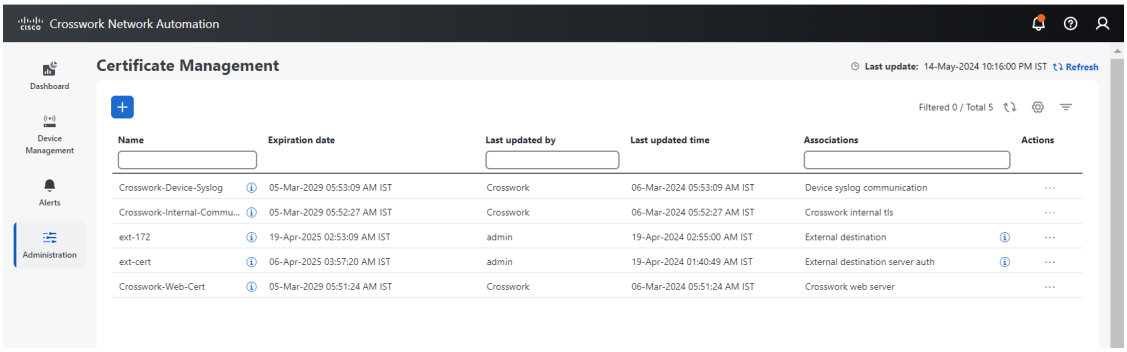


Note If gNMI certificate is already configured and you wish to onboard a device with a different trust chain, update the existing .pem file to include details of the new CA. Select the existing gNMI certificate from the list, click the Edit icon and upload the new .pem file.

Step 4 Click **Save**.

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

Figure 47: Certificates Management Window



Import and Install Certificates on Devices

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

Certificates on a Cisco IOS XR Device

To install certificates on a Cisco IOS XR device.

1. Copy rootCA.pem, device.key, and device.crt to the device under /tmp folder.
2. Log in into the IOS XR device.
3. Use the run command to enter the VM shell.

   ```
   RP/0/RP0/CPU0:xrvr-7.2.1#run
   ```
4. Navigate to the following directory:

   ```
   cd /misc/config/grpc
   ```
5. Create or replace the content of the following files:

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

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

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

Certificates on a Cisco IOS XE Device

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

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

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

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

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

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

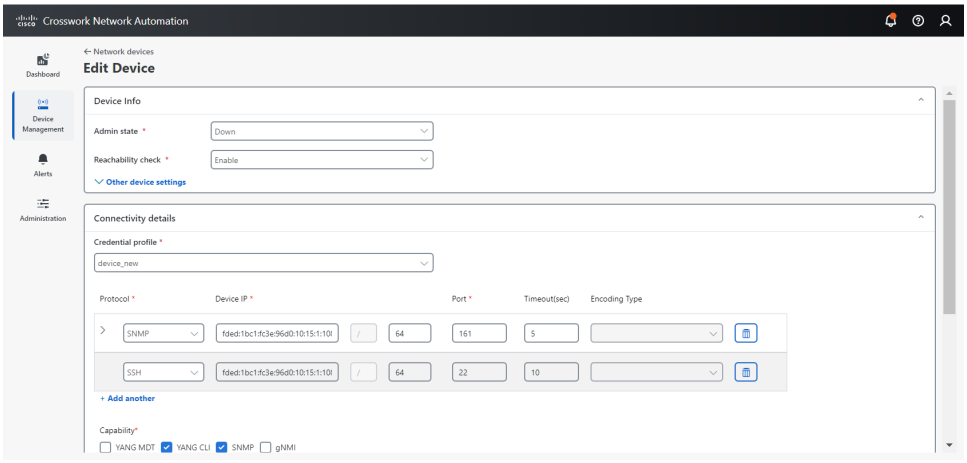
```
quit

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

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

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

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

Update Protocol on Device from Cisco Crosswork

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

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

Figure 48: Edit Device Details Window



Device Configuration for gNMI

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

Cisco IOS XR devices

1. Enable gRPC over an HTTP/2 connection.

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

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

2. Set the session parameters.

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

where:

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

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

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

Cisco IOS XE Devices

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

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

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

```
Device# configure terminal
Device(config)# gnmi-yang server
Device(config)# gnmi-yang secure-server
Device(config)# gnmi-yang secure-trustpoint trustpoint1
Device(config)# gnmi-yang secure-client-auth
Device(config)# gnmi-yang secure-port 50001 <The default port is 50051.>
```

```
Device(config)# end
Device
```

Configuring gNMI Bundling for IOS XR

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

Before you begin

Make sure that you are aware of the following:

- IOS XR release versions 7.81 and later support the gNMI bundling capability. For more information about how the bundling feature works, see Programmability Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.8.x.
- The gNMI bundling capability can only be configured from the device. This option is not available in the Crosswork Interface.

Step 1 Enable the bundling feature using the following command:

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

The gNMI bundling capability is disabled by default.

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

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

The default bundling size is 32768 bytes.

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

What to do next

Verify that the bundling capability is configured using the following:

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

Create a Collection Job from Cisco Crosswork UI

Follow the steps to create a collection job:

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

Before you begin

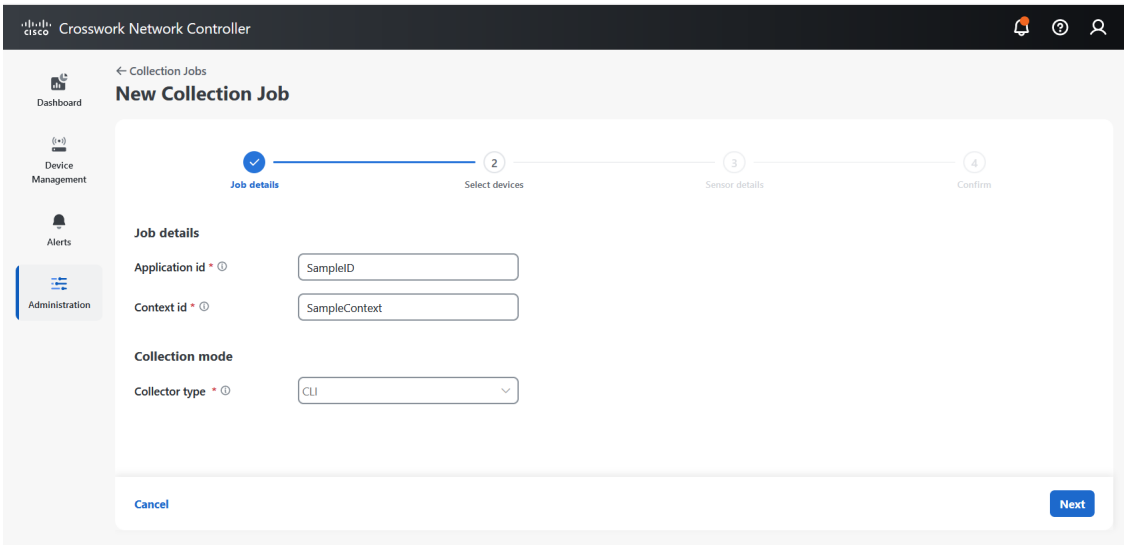
Ensure that a data destination is created (and active) to deposit the collected data. Also, have details of the sensor path and MIB that you plan to collect data from.

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

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

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

Figure 49: New Collection Job Window

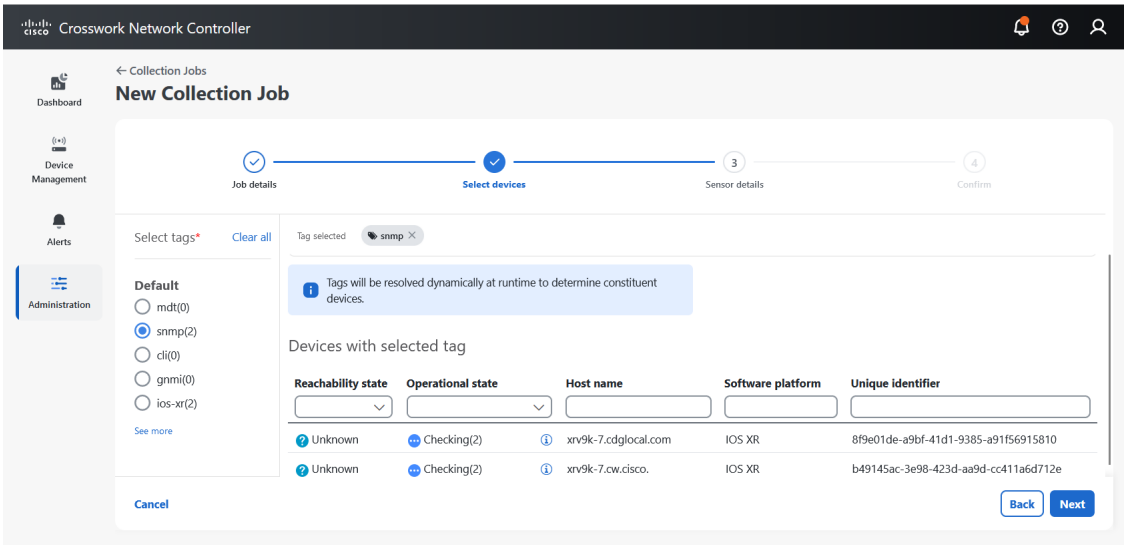


- Application Id: A unique identifier for the application.
- Context Id: A unique identifier to identify your application subscription across all collection jobs.
- Collector type: Select the type of collection - CLI or SNMP.

Click **Next**.

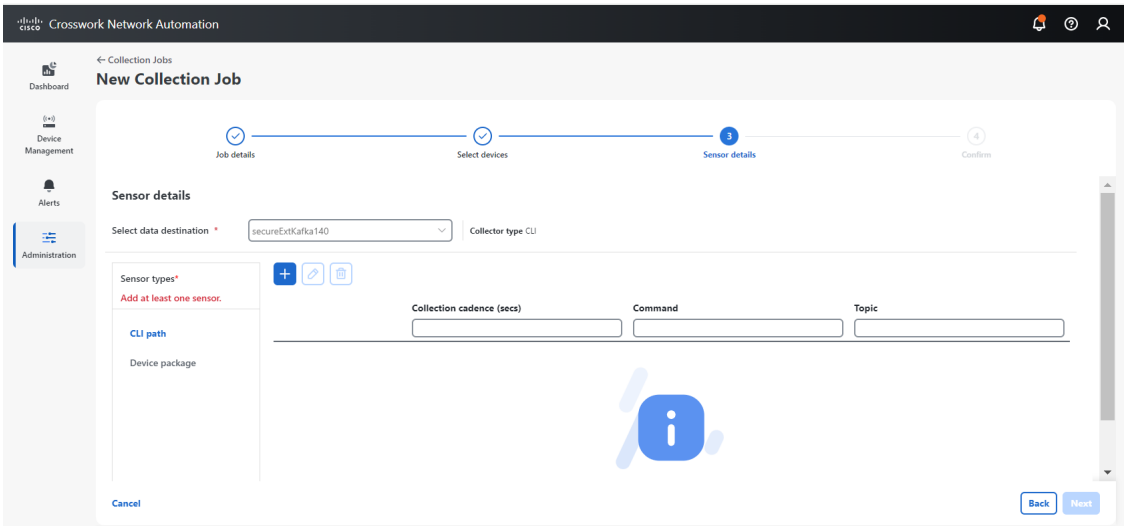
Step 4 Select the devices from which the data is to be collected. You can either select based on the device tag or manually. Click **Next**.

Figure 50: Select Devices Window



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

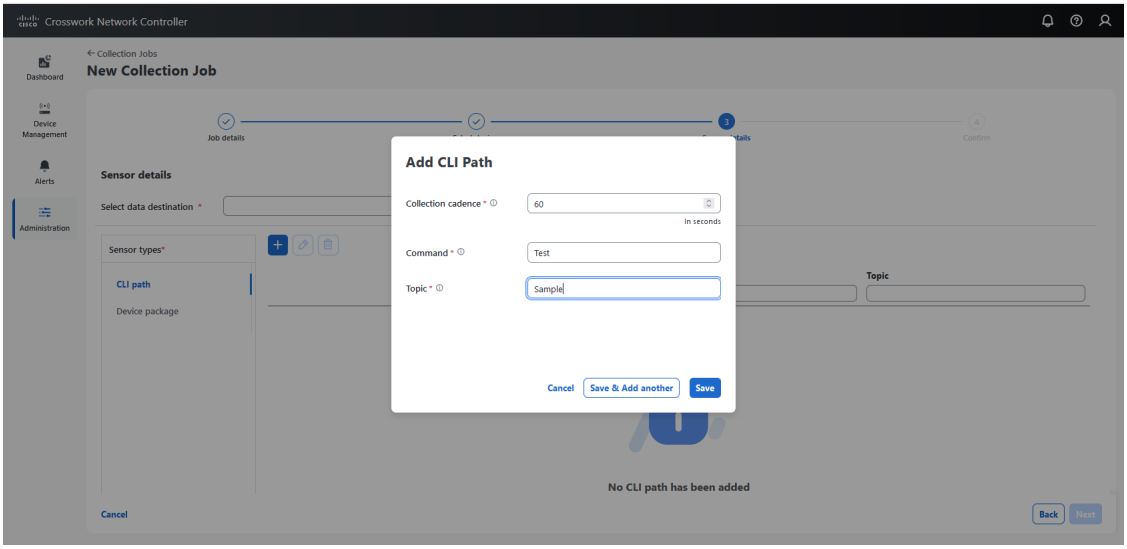
Figure 51: Sensor Details Window for CLI Path



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

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

Figure 52: Add CLI Path Dialog Box

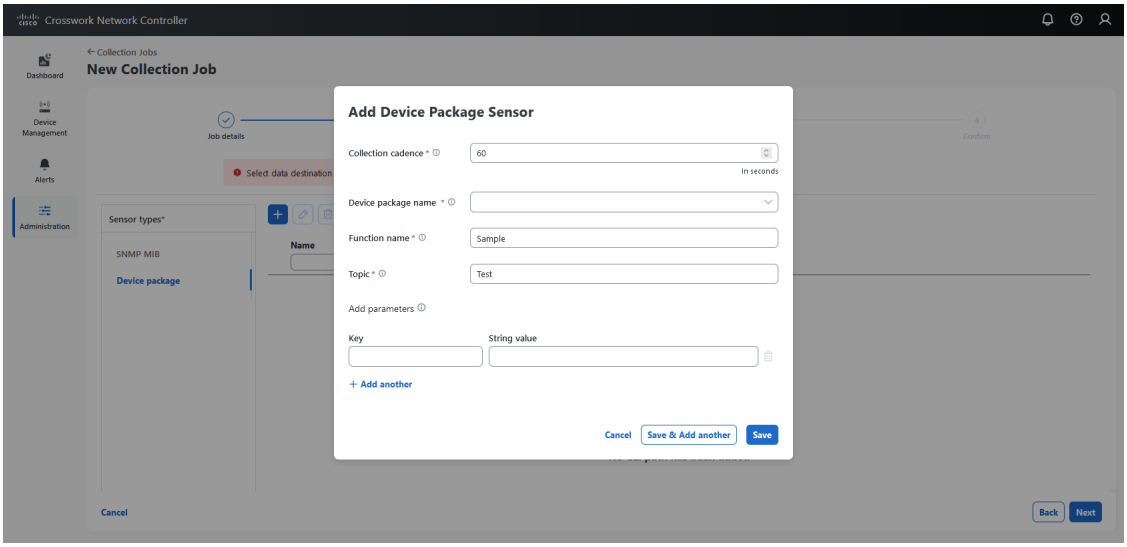


- Collection cadence: Push or poll cadence in seconds.
- Command: CLI command
- Topic: Topic associated with the output destination.

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

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

Figure 53: Add Device Package Sensor Dialog Box



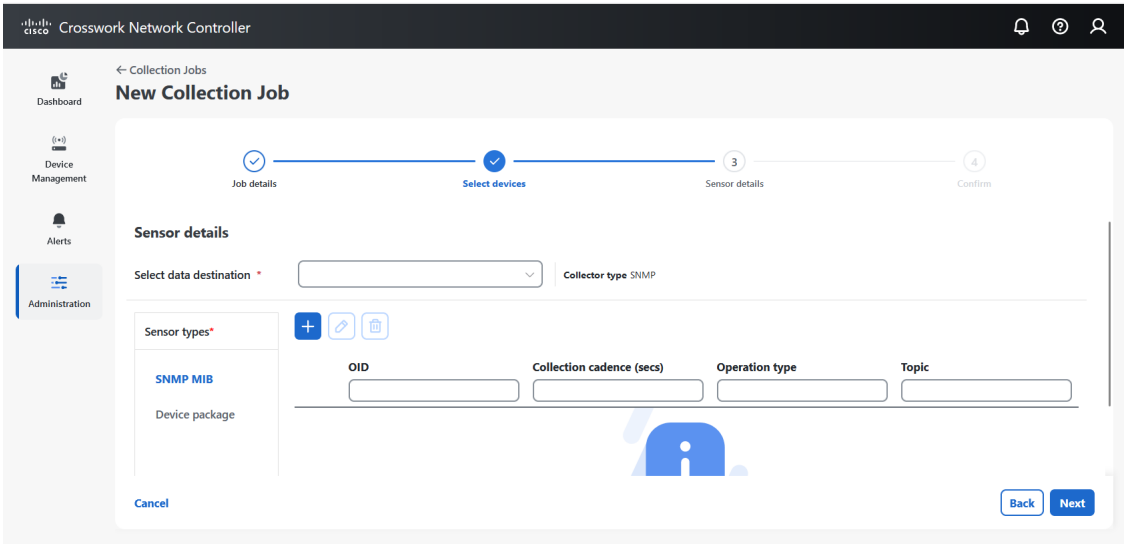
- Collection cadence: Push or poll cadence in seconds.
- Device package name: Custom XDE device package ID used while creating the device package.

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

Click **Save**.

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

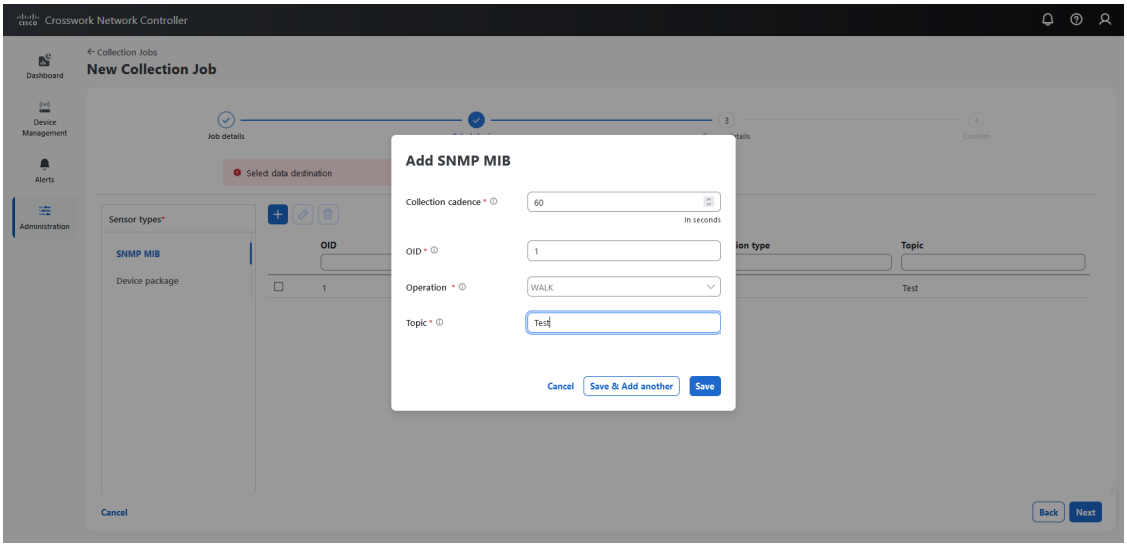
Figure 54: Sensor Details Window for SNMP Path



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

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

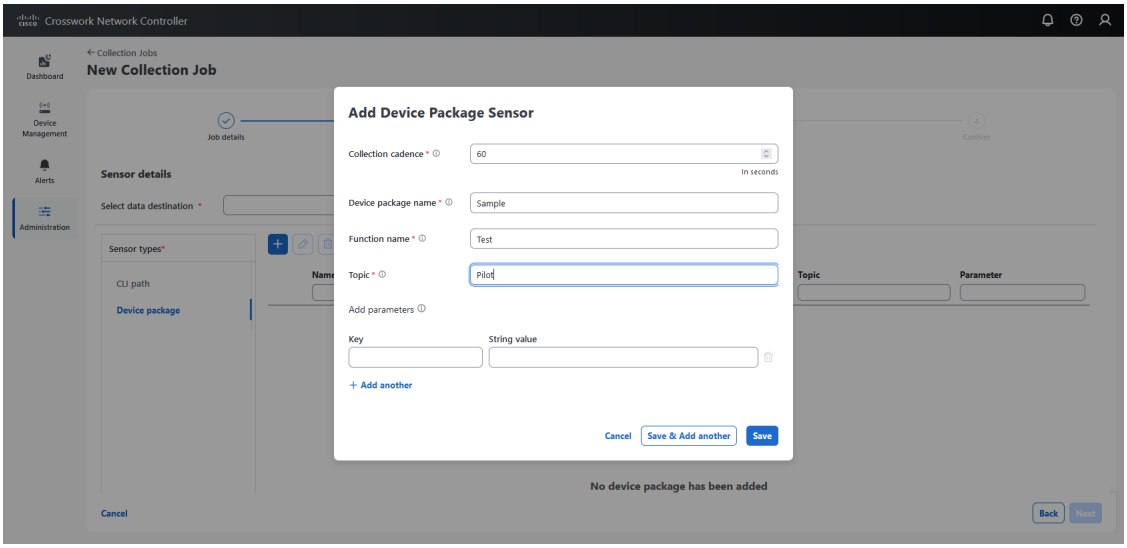
Figure 55: Add SNMP MIB Dialog Box



- Collection cadence: Push or poll cadence in seconds.
- OID
- Operation: Select the operation from the list.
- Topic: Topic associated with the output destination.

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

Figure 56: Add Device Package Sensor Dialog Box



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

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

Click **Save**.

Step 7 Click **Create Collection Job**.

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

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

```
netstat -tulpn
```

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

Monitor Collection Jobs

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

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

This left pane lists all active collection jobs along with their Status, App ID, Context ID, and Actions. The Actions drop-down lets you:

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

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

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

- Application name and context associated with the collection job.
- Status of the collection job.

Note

- The status of a collection task associated with a device after it is attached to a Crosswork Data Gateway, is **Unknown**.
- A job could have status as **Unknown** for one of the following reasons:
  - Crosswork Data Gateway has not yet reported its status.
  - Loss of connection between Crosswork Data Gateway and Cisco Crosswork.
  - Crosswork Data Gateway has received the collection job, but actual collection is still pending. For example, traps are not being sent to Crosswork Data Gateway southbound interface, or device is not sending telemetry updates.
  - The trap condition in an SNMP trap collection job which we are monitoring has not occurred. For example, if you are looking for Link Up or Link down transitions and the link state has not changed since the collector was established, then the state will report as **Unknown**. To validate that trap-based collections are working it is therefore necessary to actually trigger the trap.
- After the collection job is processed, the status changes to 'Successful' if the processing was successful or else it changes to 'Failed'.
- If a collection job is in degraded state, one of the reasons might be that the static routes to the device have been erased from Crosswork Data Gateway.
- Collections to a destination that is in an Error state do not stop. The destination state is identified in background. If the destination is in an Error state, the error count is incremented. Drill down on the error message that is displayed in the **Distribution** status to identify and resolve the issue by looking at respective collector logs.
- Cisco Crosswork Health Insights - KPI jobs must be enabled only on devices mapped to an extended Crosswork Data Gateway instance. Enabling KPI jobs on devices that are mapped to a standard Crosswork Data Gateway instance reports the collection job status as **Degraded** and the collection task status as **Failed** in the **Jobs Details** pane.

- Job configuration of the collection job that you pass in the REST API request. Click icon next to **Config Details** to view the job configuration. Crosswork Network Controller lets you view configuration in two modes:
  - View Mode
  - Text Mode
- Collection type
- Time and date of last modification of the collection job.

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

Crosswork Network Controller also displays the following details for collections and distributions:

Field	Description
Collection/Distribution Status	Status of the collection/distribution. It is reported on a on change basis from Crosswork Data Gateway. Click next to the collection/distribution status for details.
Hostname	Device hostname with which the collection job is associated.
Device Id	Unique identifier of the device from which data is being collected.
Sensor Data	Sensor path Click to see collection/distribution summary. From the sensor data summary pop up you can copy the sensor data by clicking **Copy to Clipboard**. Click to see collection/distribution metrics summary. The metrics are reported on cadence-basis i.e., once every 10 minutes by default. It shows the following metrics for a collection: • last_collection_time_msec • total_collection_message_count • last_device_latency_msec • last_collection_cadence_msec It shows the following metrics for a collection: • total_output_message_count • last_destination_latency_msec • last_output_cadence_msec • last_output_time_msec • total_output_bytes_count
Destination	Data destination for the job.

Field	Description
Last Status Change Reported Time	Time and date on which last status change was reported for that device sensor pair from Crosswork Data Gateway

Note

- `Create Failed` error means out of N devices, some devices failed to setup. However, the collection would happen on the devices that were successfully setup. You can identify the device(s) causing this error by using `Control Status` API.
- If job creation failed on a particular device because of NSO errors, after fixing NSO errors , you have to manually change the administration state of the device first to "Down" and then "Up". However, doing so resets the collection on the device.

Note Errors that occur when the creation or deletion procedure fails are displayed in a separate pop-up screen. Click next to the job status to see details of the error.

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

Collection Status for Event-based collection jobs

1. When data collection is successful, status of the Collection job changes from **Unknown** to **Success** in the **Collection Jobs** pane.
2. When a device is detached from the Crosswork Data Gateway, all corresponding collection jobs are deleted and collection job status is displayed as **Success** in the **Collection Jobs** pane. There are no devices or collection tasks displayed in the **Job Details** pane.
3. When a device is attached to a Crosswork Data Gateway, Crosswork Data Gateway receives a new collection job with the status set to **Unknown** that changes to **Success** after receiving events from the device.
4. If the device configuration is updated incorrectly on a device that is already attached to a Crosswork Data Gateway and after the Crosswork Data Gateway has received the job and events, there is no change in status of the collection task in the **Jobs Details** pane.
5. If the device inventory is updated with incorrect device IP, the collection task status in the **Jobs Details** pane is **Unknown**.

Delete a Collection Job

System jobs (default jobs created by various Crosswork Applications) should not be deleted as it causes collection issues. Jobs created by Health Insights should only be deleted by disabling the KPI profile which will remove the collection jobs it deployed. When you delete a collection job, it deletes the associated collection tasks.

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

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

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

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

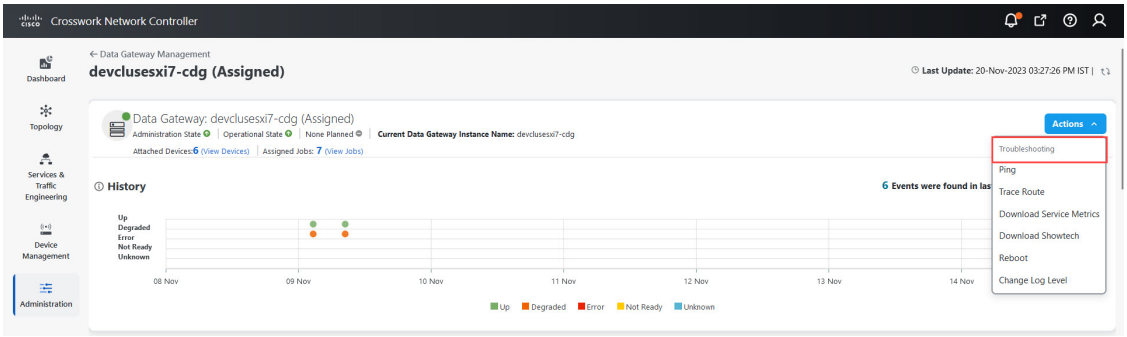
Step 4 In the corresponding row, click ⋯ and select **Delete**. The **Delete Collection Job** window is displayed.

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

Troubleshoot Crosswork Data Gateway

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

Figure 57: Data Gateway - Troubleshooting



For details on troubleshooting options available from the Interactive Console of the data gateway VM, see Troubleshooting Crosswork Data Gateway VM, on page 412.

Check Connectivity to the Destination

To check connectivity to a destination from a data gateway, use the **Ping** and **Traceroute** options from Troubleshooting Menu.

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

1. Go to **Administration** > **Data Gateway Management** > **Data gateways**.
2. Click the data gateway name from which you want to check the connectivity.
3. In the Crosswork Data Gateway details page, on the top right corner, click **Actions** and choose: **Ping** or **Traceroute**.
   - **Ping**: Enter details in the **Number of Packets**, and **Destination Address** fields and click **Ping**.

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

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

Download Service Metrics

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

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

Step 2 Click the data gateway name for which you want to download the service metrics.

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

Step 4 Enter a passphrase.

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

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

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

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

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

Download Showtech Logs

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

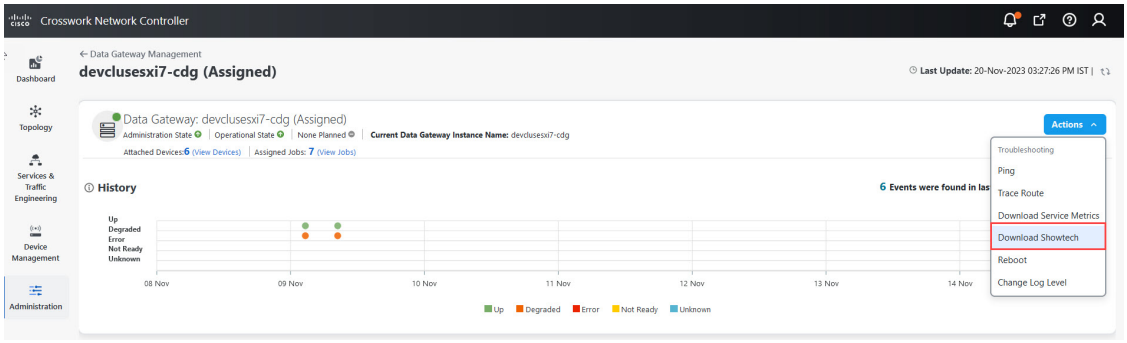
Note Showtech logs cannot be collected from the UI if the data gateway is in an ERROR state. In the DEGRADED state of data gateway, if the OAM-Manager service is running and not degraded, you will be able to collect logs.

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

Step 2 Click the data gateway name for which you want to download showtech.

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

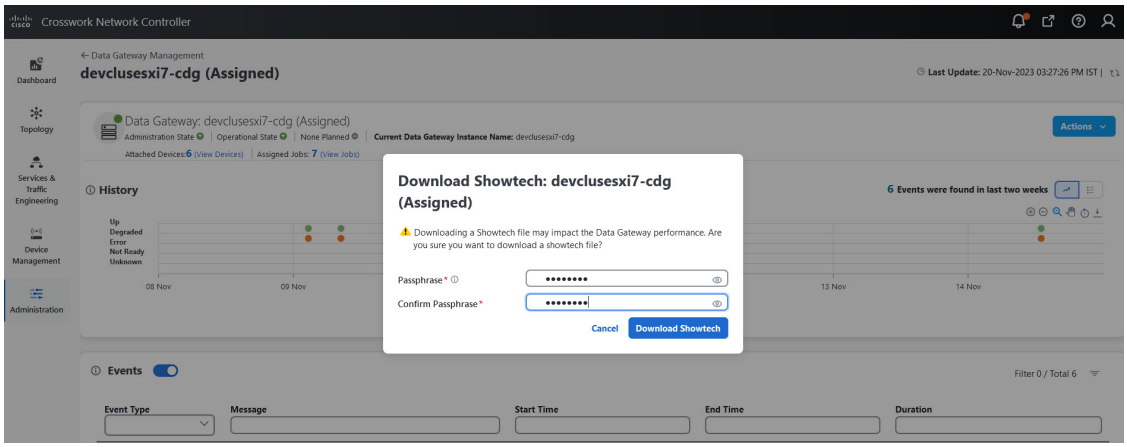
Figure 58: Data Gateway - Download Showtech



Step 4 Enter a passphrase.

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

Figure 59: Download Showtech Pop-up Window



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

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

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

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

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

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

Reboot Data Gateway VM

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

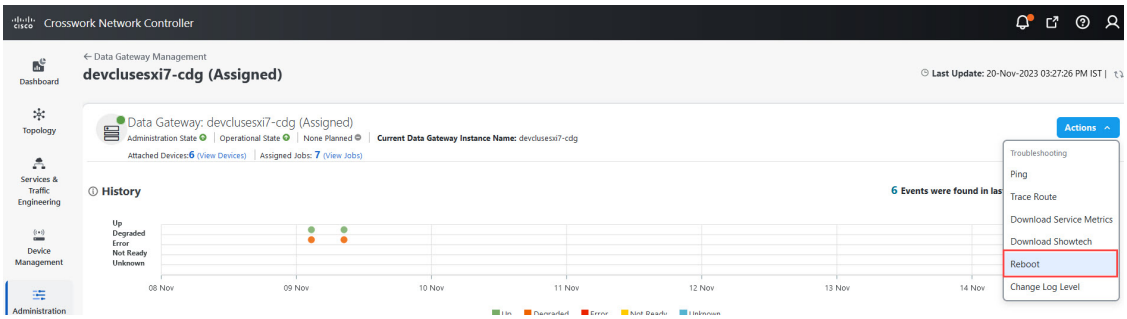
Note Rebooting the data gateway pauses its functionality until it is up again.

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

Step 2 Click the data gateway name that you want to reboot.

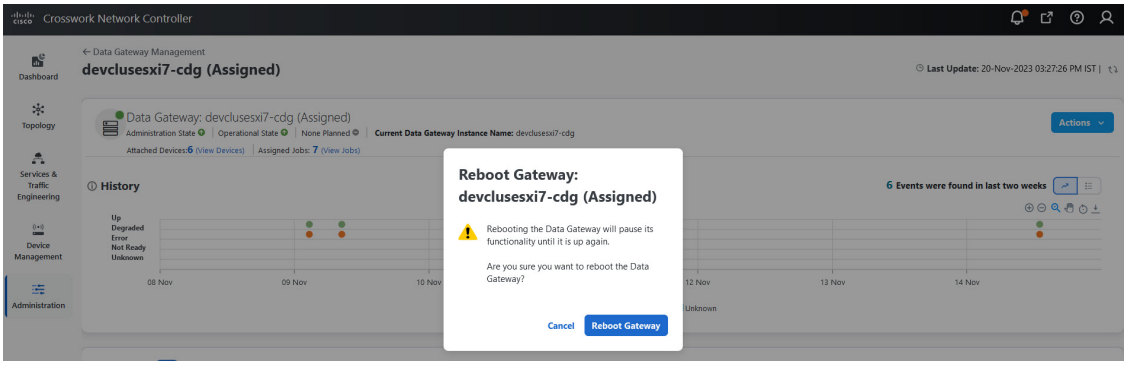
Step 3 In the Crosswork Data Gateway details page, on the top-right corner, click **Actions**, and click **Reboot**.

Figure 60: Data Gateway - Reboot



Step 4 Click **Reboot Gateway**.

Figure 61: Reboot Gateway Popup Window



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

Change Log Level of Crosswork Data Gateway Components

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

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

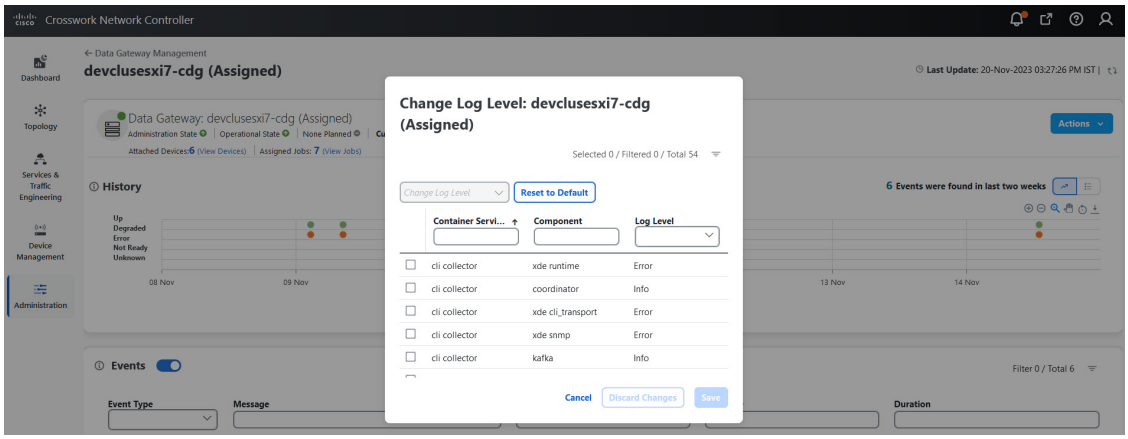
Step 1 Go to **Administration** > **Data Gateway Management** > **Data gateways**.

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

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

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

Figure 62: Change Log Level Window



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

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

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

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

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

Unable to Move Data Gateway from Assigned to Unassigned State

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

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

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

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

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

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

To resolve this issue, use the following procedure:

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

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

- Modify the NLB IP addresses and restart the Infra services (oam-manager).
- Redeploy the Crosswork Data Gateway VMs using new subnet configurations.

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

If a collection job on the Collection Jobs page is in the Degraded state, you can review the service status for more information.

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

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

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

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

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

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

Data Gateway Collects Data Despite SNMPv3 Engine ID Change

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

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

To resolve this issue, enable **Force Re-Sync USM Engine Details for SNMPV3** in the Global Parameters window or change the device admin state from DOWN to UP. For more information about enabling the resync option, see Configure Crosswork Data Gateway Global Parameters, on page 88.

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

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

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

- Reattach the devices: Attach Devices to a Crosswork Data Gateway, on page 63
- Detach the devices: Manage Crosswork Data Gateway Device Assignments, on page 71

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

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

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

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

DAD Failure Error During a Failover

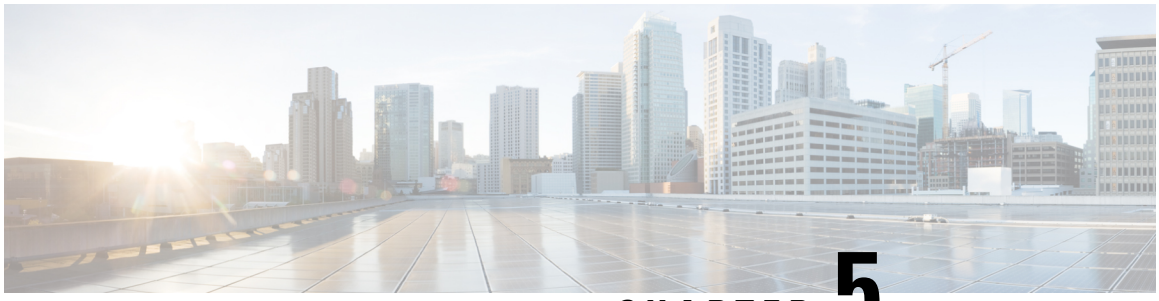
During a failover, the primary data gateway (cdg1) switches over to the secondary gateway (cdg2), and cdg2 takes on the southbound IPv6 address of cdg1. When cdg2 is detected, the Crosswok logs an event for cdg2, indicating a Duplicate Address Detection (DAD) failure due to the IP address being a duplicate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

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

Data Gateway Failover Failed

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

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



CHAPTER 5

Embedded Collectors for Single VM Deployment

The scope of this chapter is limited to Embedded Collectors used in the Crosswork Network Controller deployment on a single VM.

This section contains the following topics:

Embedded Collectors

For the single VM deployment, Crosswork Network Controller consists of the Cisco Crosswork Infrastructure, Embedded Collectors, and the Element Management Functions application bundled together in a package. For information about the single VM deployment, see *Cisco Crosswork Network Controller 7.0 Installation Guide*.

Embedded Collectors is a solution that collects network data through the collector services. The collector transfers the data to Cisco Crosswork or an external destination, or both, using either Kafka or gRPC.

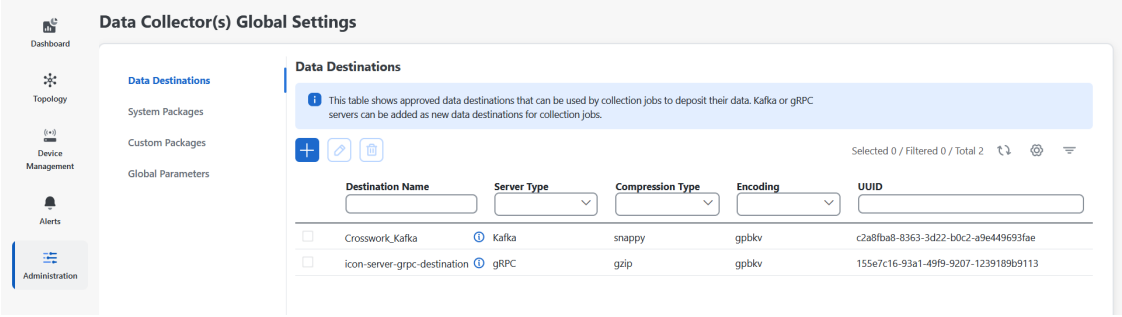
You can deploy these lightweight data collectors through the Embedded Collector and Offload Component CAPP file on the Crosswork Network Controller UI. The deployment of the CAPP file includes collectors for SNMP, gNMI, syslog, and CLI.

For information on how collectors are deployed, see *Cisco Crosswork Network Controller 7.0 Installation Guide*.

How to access the Embedded Collector UI?

To open the Embedded Collector management view, log in to Cisco Crosswork and choose **Administration** > **Data Collector(s) Global Settings** from the left navigation bar.

Figure 63: Data Collector(s) Global Settings Window



The **Data Collector(s) Global Settings** page lets you perform the administrative operations through the following menus on the left pane:

- **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.
- **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 UI allows you upload or download CLI, MIB, SNMP, and Aggregate device packages based on the type of data that you want to collect and the device.
- **Global Parameters**: The collectors UI 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 a change occurs.

Set Up Embedded Collectors to Collect Data

When does Embedded Collectors start the data collection?

The Device Lifecycle Management and Element Management Functions applications assign collection jobs to devices onboarded to the Crosswork Network Controller. This facilitates gathering essential network information and telemetry data, ensuring accurate device health reporting, and enabling the execution of other designated tasks.

How to set up Embedded Collectors?

This workflow assumes that you have already installed Embedded Collectors as explained in the *Install Cisco Crosswork Network Controller on a Single VM* chapter in *Cisco Crosswork Network Controller 7.0 Installation Guide*.

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

Table 11: Tasks to Complete to Set Up the Embedded Collectors

Task	Follow the steps in...
1. Verify that the default collection jobs are created and running successfully.	Monitor Embedded Collectors Application Health, on page 197
2. (Optional) Extend device coverage to collect data from currently unsupported devices or third-party devices.	Device Packages, on page 152
3. (Optional) Forward data to external data destinations.	Add or Edit a Data Destination, on page 146
4. (Optional) Create custom collection jobs.	Manage Collection Jobs, on page 159

Data Collector Global Configuration

This section outlines the global settings that must be configured for Embedded Collectors.

Licensing Requirements for External Collection Jobs

To set up collection jobs that send data to the external destinations, you need an 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.

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

Viewing the license status

Use these steps to view the status of your license.

1. From the main menu, go to **Administration** > **Application Management** > **Smart License**.
2. Select **Crosswork Platform Services** in the application field.
3. Ensure that the status is as follows:
   - **Registration Status** - **Registered**

     Indicates that you have registered with Cisco Smart Software Manager (CSSM) and are authorized to use the reserved licensed features.
   - **License Authorization Status** - **Authorized** (In Compliance).

     Indicates that you have not exceeded the device count in the external collection jobs.
   - Under **Smart Licensing Usage**, **CW_EXTERNAL_COLLECT** has status as **In Compliance**.

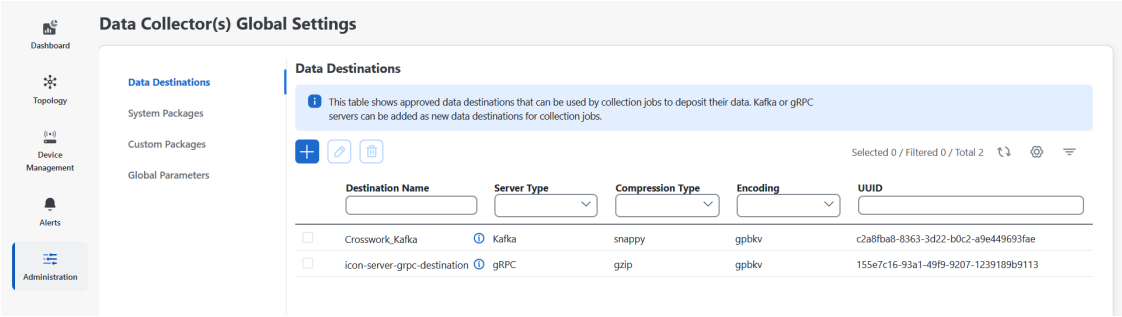
Manage External Data Destinations

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 Gateway Global Settings > 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.

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

Figure 64: Data Destinations Window



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

To view details of a data destination, in the **Data Destinations** pane, click the icon next to the data destination name whose details you want to view. See View Data Destination Details, on page 151 for more information.

Add or Edit a Data Destination

Before you begin

When configuring an external Kafka server for data collection, ensure the following:

- The following properties are configured on the external Kafka server:

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

  - `num.io.threads = 8`
  - `num.network.threads = 3`

- `message.max.bytes= 30000000`

- The necessary Kafka topics for data collection are created according to your preferences.
- The Kafka destination is configured with the 'reachability-topic' prior to initiating a new collection job. To monitor the health of the Kafka destination, this configuration is necessary.
- You can add multiple data destinations.
- If you reinstall an already existing external Kafka data destination with the same IP address, the collectors must be restarted for changes to take effect.
- You can secure the communication channel between Crosswork and the specified data destination that is, either Crosswork Kafka or external Kafka. (See **Step 6** in this procedure). However, enabling security can impact performance.
- If your external data destination requires a TLS connection, keep the public certificate ready or if it requires client authentication, keep the client certificate and key files ready. The client key might be password-encrypted which needs to be configured as part of the data destination provisioning. Currently, Embedded Collectors support IP-based certificates only.
- Ensure that the certificates are PEM encoded and the key file is in PKCS#8 format when generating them with your Certificate Authority.
- Ensure that you create the Kafka topics before you submit the job to Crosswork. Depending on the external Kafka and how topics are managed in that external Kafka, Crosswork logs may show the following exception if the topic does not exist at the time of dispatching the collected data to that specific external Kafka/topic. This could be because the topic is not created yet or the topic was deleted before the collection job was complete.

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

- Check and validate the port connectivity for the data destination. If the port is unreachable in the destination, it leads to a failed collection.
- Embedded Collectors allows you to configure custom values in the destination properties for a Kafka destination (see **Step 4** in this procedure).

Note This feature is not supported on a gRPC destination.

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

Follow these steps to add a new or modify a data destination. The Embedded Collectors will send the collected data to this destination.

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

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

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

Note When you update a data destination, the collector using it will need to establish a new session with that destination. The collection of data will pause and continue once the session is restored.

Step 3 Enter or update these values as per the requirements from your external data destination. If values are not provided, consider using the defaults as a starting point.

Field	Value	Available in gRPC	Available in Kafka
Destination Name	Enter a descriptive data destination name. The name can contain a maximum of 128 alphanumeric characters, plus underscores ("_") or hyphens ("-"). No other special characters are allowed. If you have many data destinations, make the name as informative as possible to be able to distinguish later.	Yes	Yes
Server Type	From the drop-down, select the server type of your data destination.	Yes. Select gRPC	Yes. Select Kafka
Encoding	From the drop-down, select the encoding (json or gpbkv).	Yes	Yes
Compression Type	From the drop-down, select the compression type. gRPC supports snappy, gzip, lz4, zstd, and none. Kafka supports snappy, gzip, and deflate. The zstd compression type is supported only for Kafka 2.0 or higher.	Yes	Yes
Maximum Message Size (bytes)	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
Buffer Memory	Enter the required buffer memory in bytes. • **Default Value**: 52428800 bytes/ 52.4288 MB • **Min**: 52428800/ 52.4288 MB bytes • **Max**: 314572800 bytes/ 314.5728 MB	No	Yes

Field	Value	Available in gRPC	Available in Kafka
Batch Size (bytes)	Enter the required batch size in bytes. • **Default Value**: 6400000 bytes/6.4 MB • **Min**: 16384 bytes/ 16.38 KB • **Max**: 314572800 bytes/ 314572.8 KB	No	Yes
Linger (milliseconds)	Enter the required linger time in milliseconds. • **Default Value**: 5000 ms • **Min**: 0 ms • **Max**: 5000 ms	No	Yes
Request Timeout	Enter the duration that the request waits for a response. After the configured duration is met, the request expires. • **Default Value**: 30 seconds • **Min**: 30 seconds • **Max**: 60 seconds	Yes	Yes

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

Step 4 (Optional) To configure custom values that are different from global properties for a Kafka destination, in the **Collectors - Custom Properties** pane:

a) Select a **Collector**.

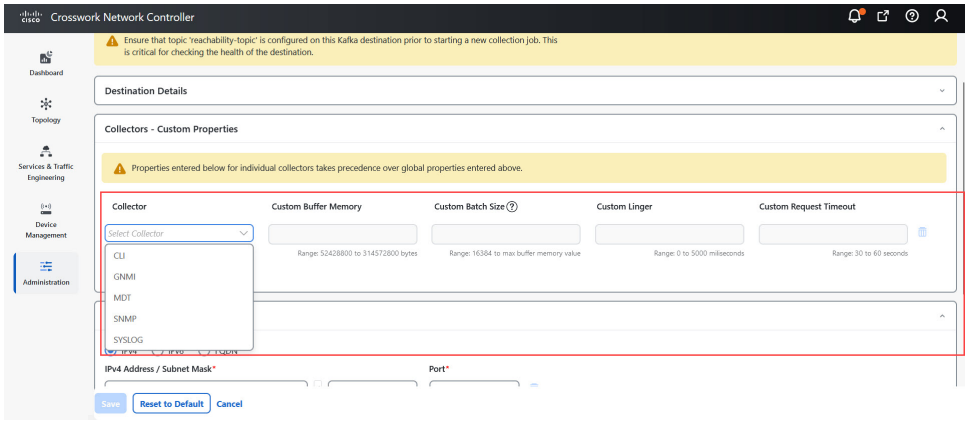
b) Enter values for the following fields:

- **Custom Buffer Memory**
- **Custom Batch Size**

  Note The **Custom Batch Size** cannot exceed the value of the **Custom Buffer Memory** at run time. In the 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 65: Add Destination Window



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

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

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

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

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

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

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

Connectivity Type	Fields	Available in gRPC	Available in Kafka
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**. Make sure the firewall does not block the chosen port.	Yes	Yes

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

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

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

- **Mutual-Auth**: Authenticates external server and Embedded Collectors after the CA certificate, and Intermediate certificate or Key is uploaded to the Crosswork UI.
- **Server-Auth**: Authenticates external server and Embedded Collectors after the CA certificate is uploaded to the Crosswork UI. **Server-Auth** is the default authentication process.

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

Step 9 Click **Save**.

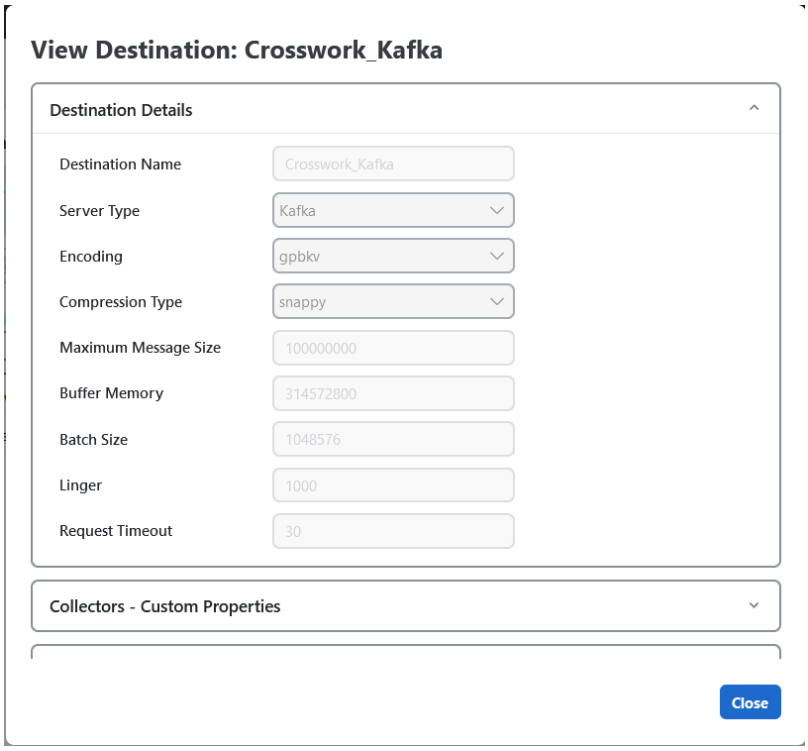
What to do next

If you have enabled the **Enable Secure Communication** option, navigate to the **Certificate Management** page in the Cisco Crosswork UI (**Administration > Certificate Management**) and add the relevant certificate for the newly added data destination. This step is mandatory to establish a secure communication to the device. See Manage Certificates, on page 289 for more information.

Important If certificate is not added or the certificate is incomplete for the data destination after enabling the **Enable Secure Communication** option, Cisco Crosswork sets the destination to an error state. When the destination is in an error state, the collection job status will be degraded.

View Data Destination Details

To view details of a data destination, in the **Data Destinations** pane, click icon next to the data destination name whose details you want to see. Crosswork Network Controller displays the detailsas shown in the following figure.



Delete a Data Destination

Follow the steps to delete a data destination:

Before you begin

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

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

Step 2 Select one or more data destinations that you want to delete from the list of destinations that is displayed and click the button.

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

Device Packages

Device management enables the embedded collectors to extend the data collection capabilities to the Cisco applications and third-party devices through the device packages. The Embedded Collectors supports system and custom device packages.

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

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

How to access the device packages

Access the **Packages** pane from **Administration > Data Collector(s) Global Settings**. Choose **System packages** or **Custom packages**.

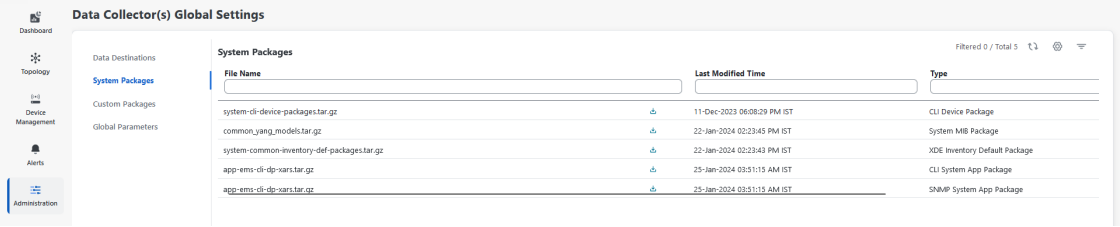
System Packages

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

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

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

Figure 66: System Packages Window



Download System Packages

To download a system package, from the main menu, choose **Administration** > **Data Collector(s) Global Settings** > **System Packages**. Click on the button next to the package name in the **File Name** column.

Custom Packages

You can upload the following types of custom packages to Cisco Crosswork:

1. **CLI Device Package**: The CLI-based KPIs are used to monitor device health for third-party devices. All custom CLI device packages along with their corresponding YANG models should be included in the `custom-cli-device-packages.tar.xz` file. Multiple files are not supported. However, you can use the aggregate package if you want to bundle different files for different devices in a single package.
2. **Custom MIB Packages**: Custom MIBs and device packages can be customized to third-party devices. They are used to filter the collected data or format it differently for Cisco devices. These packages can be edited. All custom SNMP MIB packages along with YANG models should be included in file `custom-mib-packages.tar.xz`. Crosswork does not support multiple Custom MIB package.

Note The Embedded Collectors enable SNMP polling on third-party devices for standard MIBs that are already included in the system. Proprietary MIBs are required only if the collection request references MIB TABLE names or SCALAR names from a proprietary MIB. However, if the requests are OID-based, the MIBs are not required.

3. **SNMP Device Package**: The Embedded Collectors allow you to extend the SNMP coverage by uploading custom SNMP device packages with any additional MIB and YANG descriptions you require.
4. **Aggregate Package**: With the aggregate package, you have the option to include multiple supported file extensions in a single package. The Crosswork UI allows you to either upload or download these packages. Each package may contain one or multiple files with the following extensions:

   Collector files

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

   Application files

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

Add Custom Packages

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

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

Note Crosswork Network Controller does not validate the files being uploaded other than checking the file extension.

Follow these steps to upload a custom software package:

Before you begin

- When uploading new MIBs as a part of the Custom MIB Package, ensure that those new MIBs files can be uploaded within collectors along with the existing System MIB files that are, all dependencies in the files are resolved properly.
- If you plan on adding an Aggregate package, ensure that:
  - The package must contain only supported file extensions. For a list of supported extensions, see Custom Packages, on page 153.

- The files must only be bundled in the .tar.gz format.
- The top-level directory must contain at least one of the specified collector types:
  - snmp
  - cli
  - common

Sample directory structure:

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

```
│   └── snmp-xar2.xar
└── yangs
    ├── snmp-yang1.yang
    └── snmp-yang2.yang
```

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

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

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

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

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

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

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

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

Step 6 Click **Upload**.

What to do next

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

Delete Custom Package

When you remove a custom package from Cisco Crosswork, all YANG and XAR files are automatically deleted. Removing custom packages affects all collection tasks that rely on the custom package.

Follow the steps to delete a custom package:

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

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

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

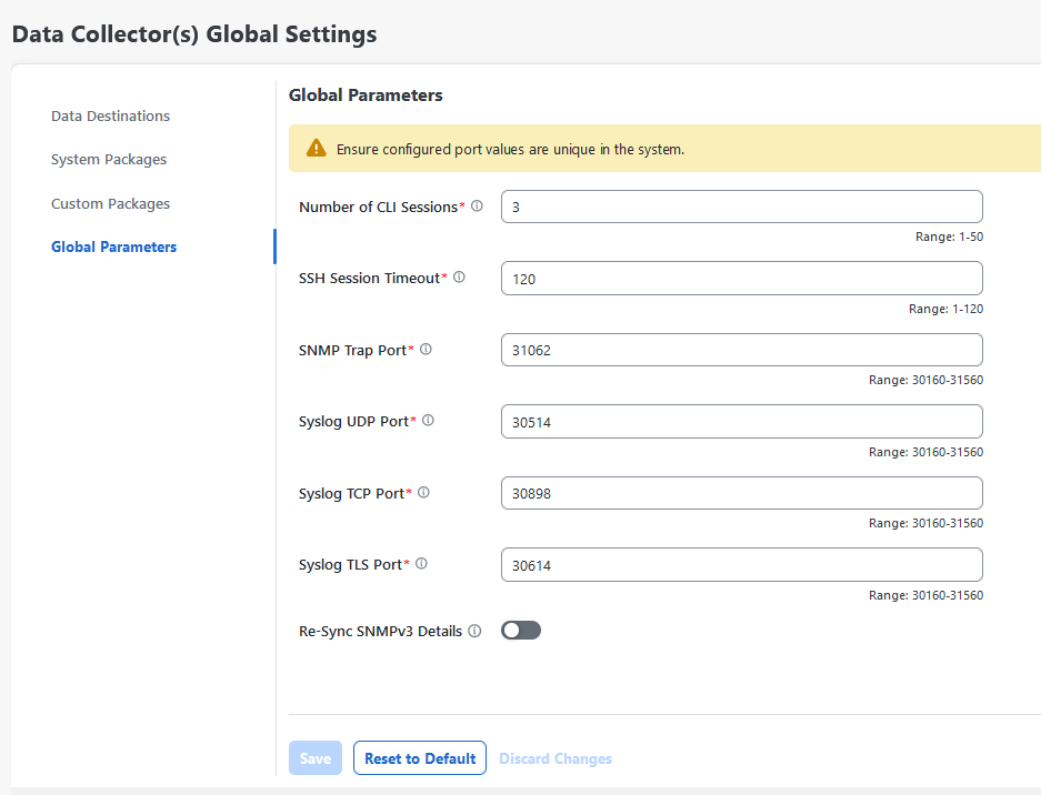
Configure Global Parameters

The **Global Parameters** window allows you to update the port across all the data collectors in the network.

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

Step 1 From the main menu, navigate to **Administration > Data Collector(s) Global Settings > Global Parameters**.

Figure 67: Global Parameters Window



Step 2 Change one of more of the following parameters.

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

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. **Note** This value overrides any internal configuration set for the same parameter.	3 Accepted range is 1-50
SSH Session Timeout	The session timeout (in seconds) is the duration for which a CLI connection can remain idle in the CLI and SNMP collectors.	120 Accepted range is 1-120 seconds

Parameter Name	Description	Default value for single VM deployment
SNMP Trap Port	Modify this value as per your deployment environment and configuration requirements.	31062 Accepted range is 30160–31560
Syslog UDP Port	Modify this value as per your 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
Re-Sync SNMPv3 Details	USM details change whenever a device is rebooted or reimaged. SNMPV3 collections stop working whenever there is a change in any of the USM details. Enable the option to synchronize the USM details automatically whenever there is a change following the initial collection failure. By default, the option is disabled.	Disable

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

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

A window appears indicating if the parameters update on embedded data collectors in the network was successful or not.

1. If all the embedded data collectors were updated successfully, a success message appears in the UI indicating that the update was successful.
2. If any of the embedded data collectors in the network could not be updated, an Error window appears in the UI. The embedded data collectors will automatically try to update the parameters on the failed embedded data collectors during recovery. Some of the collectors might be restarted as part of the recovery.

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

Manage Collection Jobs

Applications request data collection via the collection jobs. Subsequently, Cisco Crosswork assigns these collection jobs to a collector who handles the request. The collector starts the data collection depending on the type of data to be collected.

Embedded Collectors are capable of collecting data using protocols such as CLI, SNMP, gNMI (dial-in), and syslog. The collectors can collect any type of data as long as they can forward it over one of the supported protocols.

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

1. Data collection request to forward data for internal processes within Cisco Crosswork. Cisco Crosswork creates system jobs for this purpose. If you want the data gateway to collect specific information from non-Cisco devices, you must use custom device packages. For more information on custom device packages, see Custom Packages, on page 153.

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

2. Data collection request to forward data to an external data destination. For more information on configuring the external data destinations (Kafka or gRPC), see Manage External Data Destinations, on page 146.

You can forward collected data to an external data destination and Crosswork Network Controller in a single collection request.

You can view collection jobs currently active from the **Collection Jobs** page.

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

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

Types of Collection Jobs

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

- CLI Collection Job, on page 160
- SNMP Collection Job, on page 161
- Syslog Collection Job, on page 168
- gNMI Collection Job, on page 178

For each collection job that you create, Embedded Collectors execute the collection request and forwards the collected data to the specified data destination.

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

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

The **Cadence** value determines the frequency at which Embedded Collectors collect the data from the device. You can set the frequency between 10 and 604800000 milliseconds. We recommend a cadence of minimum 60 milliseconds.

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

Note When collection from a device is skipped due to a previous execution still in progress, Embedded Collectors raise a warning log. No alert is generated for this scenario.

CLI Collection Job

Embedded Collectors support CLI-based data collection from the network devices. Following commands are supported for this type of collection job:

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

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

You can create a CLI collection job from the Cisco Crosswork UI or using APIs. For information on creating jobs through the UI, see Create a Collection Job from Cisco Crosswork UI, on page 125and from API, see Cisco DevNet for more information.

Sample payload of CLI collection job

In this example, Crosswork sends the data to an external Kafka destination, including the UUID used by the device:

1. The device is identified with a UUID rather than an IP address.
2. The destination is also referenced by a UUID. For collections jobs built using the UI, Cisco Crosswork looks up the UUIDs. When you create your own collection jobs, you will need to look up these values.

```
{
  "collection_job": {
    "application_context": {
      "context_id": "collection-job1",
      "application_id": "APP1"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "CLI_COLLECTOR"
    },
    "job_device_set": {
      "device_set": {
        "devices": {
```

```
        "device_ids": [
          "658adb03-cc61-448d-972f-4fcec32cbfe8"
        ]
      }
    }
  },
  "sensor_input_configs": [
    {
      "sensor_data": {
        "cli_sensor": {
          "command": "show platform"
        }
      },
      "cadence_in_millisec": "60000"
    }
  ],
  "sensor_output_configs": [
   {
      "sensor_data": {
        "cli_sensor": {
          "command": "show platform"
        }
      },
      "destination": {
        "destination_id": "1e71f2fb-ea65-4242-8efa-e33cec71b369",
        "context_id": "topic1"
      }
    }
  ]
 }
}
```

SNMP Collection Job

Embedded Collectors support SNMP-based data collection based on the OIDs supported on the devices. The SNMP OID-based collection jobs can be created from the Cisco Crosswork UI or using the API, and SNMP-traps using the API.

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

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

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

The device packages can be imported into the Embedded Collectors instance as described in Section Add Custom Packages, on page 85.

Supported SNMP versions for data polling and traps are:

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

- Supported auth protocols – SHA-1, MD5
- Supported priv protocols – AES-128, AES-192, AES-256, CiscoAES192, CiscoAES256, DES, and 3-DES.

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

Sample Configurations on Device:

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

Table 12: Sample configuration to enable SNMP on device

Version	Command	To...
V2c	`snmp-server group <group_name> v2c` `snmp-server user <user_name> <group_name> v2c`	Define the SNMP version, user/user group details.
	`snmp-server host <host_ip> traps SNMP version <community_string> udp-port 31062` `snmp-server host a.b.c.d traps version 2c v2test udp-port 31062`	Define the destination to which trap data must be forwarded. **Note** The IP address mentioned here must be the virtual IP address of Embedded Collectors.
	`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 31062`	Define the destination to which trap data must be forwarded. **Note** The IP address mentioned here must be the virtual IP address of Embedded Collectors.
	`snmp-server user <user_name> <group_name> v3 auth md5 <password> priv aes 128 <password>`	Configures the SNMP server group to enable authentication for members of a specified named access list.
	`snmp-server view <user_name> < MIB > included`	Define what must be reported.
	`snmp-server group <group_name> v3 auth notify <user_name> read <user_name> write <user_name>`	Define the SNMP version, user/user group details.
	`snmp-server enable traps snmp [authentication ] [linkup ] [linkdown ] [warmstart ] [coldstart ]`	• When used without any of the optional keywords, enables authenticationFailure, linkUp, linkDown, warmStart, and coldStart traps. • When used with keywords, enables only the trap types specified. For example, to globally enable only linkUp and linkDown SNMP traps for all interfaces, use the **snmp-server enable traps snmp linkup linkdown** form of this command.

The SNMP Collector supports the following operations:

- SCALAR

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

- TABLE
- WALK
- COLUMN

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

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

The value for snmpRequestTimeoutMillis should be specified in milliseconds:

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

The following is an SNMP collection job sample:

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

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

SNMP Traps Collection Job

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

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

Embedded Collectors listen on UDP port 31062 for Traps.

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

SNMP Trap Collection Job Workflow

On receiving an SNMP trap, :

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 UI. For more information about this option, see Add Devices Through the User Interface, on page 282.

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

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

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

If the collection job is invalid, there is a missing configuration on the device, or no trap is received, the status of the job remains "Unknown". For list of supported Traps and MIBs, see List of Pre-loaded Traps and MIBs for SNMP Collection, on page 421.

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

Table 13: List of Supported Non-Yang/OID based Traps

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

Following is an SNMP-Trap collection job sample:

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

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

Enabling Traps forwarding to external applications

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

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

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

- Link up

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.4
  ```

- Link Down

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.3
  ```

- Syslog

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.4.1.9.9.41.2.0.1
  ```

- Cold Start

  ```
  1.3.6.1.6.3.1.1.4.1.0 = 1.3.6.1.6.3.1.1.5.1
  ```

```
{
  "nodeIdStr": "BF5-XRV9K1.tr3.es",
  "nodeIdUuid": "C9tZ5lJoSJKf5OZ67+U5JQ==",
  "collectionId": "133",
  "collectionStartTime": "1580931985267",
  "msgTimestamp": "1580931985267",
  "dataGpbkv": [
    {
      "timestamp": "1580931985267",
      "name": "trapsensor.path",
      "snmpTrap": {
        "version": "V2c",
```

```
          "pduType": "TRAP",
          "v2v3Data": {
            "agentAddress": "172.70.39.227",
            "oidRecords": [
              {
                "oid": "1.3.6.1.2.1.1.3.0",
                "strValue": "7 days, 2:15:17.02"
              },
              {
                "oid": "1.3.6.1.6.3.1.1.4.1.0",  // This oid is the Object Identifier.
                "strValue": "1.3.6.1.6.3.1.1.5.3" // This is the value that determines the
kind of trap.
              },
              {
                "oid": "1.3.6.1.2.1.2.2.1.1.8",
                "strValue": "8"
              },
              {
                "oid": "1.3.6.1.2.1.2.2.1.2.8",
                "strValue": "GigabitEthernet0/0/0/2"
              },
              {
                "oid": "1.3.6.1.2.1.2.2.1.3.8",
                "strValue": "6"
              },
              {
                "oid": "1.3.6.1.4.1.9.9.276.1.1.2.1.3.8",
                "strValue": "down"
              }
            ]
          }
        }
      }
    ],
    "collectionEndTime": "1580931985267",
    "collectorUuid": "YmNjZjEzMTktZjFlOS00NTE5LWI4OTgtY2Y1ZmQxZDFjNWExOlRSQVBfQ09MTEVDVE9S",
    "status": {
      "status": "SUCCESS"
    },
    "modelData": {},
    "sensorData": {
      "trapSensor": {
        "path": "1.3.6.1.6.3.1.1.5.4"
      }
    },
    "applicationContexts": [
      {
        "applicationId": "APP1",
        "contextId": "collection-job-snmp-traps"
      }
    ]
}
```


Syslog Collection Job

Embedded Collectors supports syslog-based events collection from devices.

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

The following syslog formats are supported:

- RFC5424 syslog format
- RFC3164 syslog format

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

While the order of the configuration steps does not matter, you must complete both the steps, or no data will be sent or collected. For sample device configuration, see Configure Non-secure Syslog on Device, on page 109. Cisco Crosswork also allows you to set up secure syslog communication to the device. For more information, see Configure Secure Syslog on Device, on page 111.

Sample Syslog collection payload

This is a sample syslog collection payload:

```
{
  "collection_job": {
      "job_device_set": {
      "device_set": {
        "devices": {
          "device_ids": [
            "c6f25a33-92e6-468a-ba0d-15490f1ce787"
          ]
        }
      }
    },
    "sensor_output_configs": [
      {
        "sensor_data": {
          "syslog_sensor": {
            "pris": {
                "facilities": [0, 1, 3, 23,4],
                "severities": [0, 4, 5, 6, 7]
            }
        }
        },
        "destination": {
          "context_id": "syslogtopic",
          "destination_id": "c2a8fba8-8363-3d22-b0c2-a9e449693fae"
        }
      }
    ],
    "sensor_input_configs": [
      {
        "sensor_data": {
          "syslog_sensor": {
            "pris": {
                "facilities": [0,1, 3, 23,4],
                "severities": [0,4, 5, 6, 7]
            }
        }
        },
        "cadence_in_millisec": "60000"
      }
    ],
```

```
    "application_context": {
      "context_id": "demomilesstone2syslog",
      "application_id": "SyslogDemo2"
    },
    "collection_mode": {
      "lifetime_type": "APPLICATION_MANAGED",
      "collector_type": "SYSLOG_COLLECTOR"
    }
  }
}
```

- You can filter the output of syslog data collection by specifying either PRI-based SyslogSensor OR Filters-based SyslogSensor. The syslog events matching the facilities and severities mentioned in the payload are sent to the specified destination. All other nonmatching syslog events are dropped. You can specify the filter based on regEx, severity, or facility.
- If you have specified values for severity and facility, then both the conditions are combined based on the logical operator specified at Filters level.
- You can specify a maximum of three filters combinations using the logical operator AND or OR. By default, the AND operator is applied if do not specify an operator.

Syslog Collection Job Output

When you onboard a device from Crosswork Network Controller UI (**Device Management > Network Devices > Device Details**), the value you choose in the **Syslog Format** field configures the format in which syslog events received from the device should be parsed by the syslog collector. You can choose either **UNKNOWN**, **RFC5424** or **RFC3164**.

Following is the sample output for each of the options:

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

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

Sample output:

```
node_id_str: "xrv9k-VM8"
node_id_uuid: ":i\300\216>\366BM\262\270@\337\225\2723&"
collection_id: 1056
collection_start_time: 1616711596200
msg_timestamp: 1616711596201
data_gpbkv {
  timestamp: 1616711596201
  name: "syslogsensor.path"
  fields {
    name: "RAW"
    string_value: "<6>1 Mar 25 15:34:41.321 PDT - SSHD_ 69570 - - 98949:
RP/0/RP0/CPU0:SSHD_[69570]: %SECURITY-SSHD-6-INFO_SUCCESS : Successfully authenticated
user \'admin\' from \'40.40.40.116\' on \'vty0\'(cipher \'aes128-ctr\', mac \'hmac-sha1\')
 \n"
  }
  fields {
    name: "DEVICE_IP"
    string_value: "40.40.40.30"
  }
}
```

```
collection_end_time: 1616711596200
collector_uuid: "17328736-b726-4fe3-b922-231a4a30a54f:SYSLOG_COLLECTOR"
status {
  status: SUCCESS
}
model_data {
}
sensor_data {
  syslog_sensor {
    pris {
      facilities: 0
      facilities: 3
      facilities: 4
      facilities: 23
      severities: 0
      severities: 5
      severities: 6
      severities: 7
    }
  }
}
application_contexts {
  application_id: "SyslogApp-xr-8-job1"
  context_id: "xr-8-job1"
}
version: "1"
```

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

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

RFC5424

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

Sample output:

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

```
      string_value: "172.28.122.254"
    }
  }
  collection_end_time: 1596306752742
  collector_uuid: "ac961b09-8f67-4c93-a99a-31eef50f7fa9:SYSLOG_COLLECTOR"
  status {
    status: SUCCESS
  }
  ....
  ....
```

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

Configure Non-Secure Syslog on Device

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

Note The syslog format that you configure for the device must match the format that you specified when the device was added through the Crosswork UI. See Add Devices Through the User Interface, on page 282 for more information.

Configure RFC3164 Syslog format

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

For IOS XR:

```
logging <CDG IP> port 30514 OR logging <CDG 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>
```

For IOS XE:

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

Configure RFC5424 Syslog format

For IOS XR:

```
logging <CDG 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
```

For IOS XE:

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

Configure Secure Syslog on Device

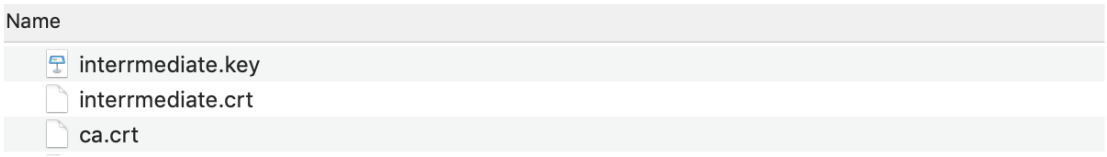
Use the steps to establish a secured syslog communication with the device.

1. Download the Cisco Crosswork trust chain from the **Certificate Management UI** page in Cisco Crosswork.
2. Configure the device with the Cisco Crosswork trustchain.

Download Syslog Certificates

1. In the Cisco Crosswork UI, go to **Administration > Certificate Management**.
2. Click *i* in the **crosswork-device-syslog** row.
3. Click **Export All** to download the certificates.

   The following files are downloaded to your system.



Configure Cisco Crosswork Trustpoint on Device

Sample IOS XR device configuration to enable TLS

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


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

-----BEGIN CERTIFICATE-----
MIIGKzCCBBOgAwIBAgIRAKfyU89yjmrXVDRKBWuSGPgwDQYJKoZIhvcNAQELBQAw
bDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMREwDwYDVQQHEwhTYW4gSm9zZTEa
```

```
.....................................................................
.....................................................................
jPQ/UrO8N3sC1gGJX7CIIh5cE+KIJ51ep8i1eKSJ5wHWRTmv342MnG2StgOTtaFF
vrkWHD02o6jRuYXDWEUptDOg8oEritZb+SNPXWUc/2mbYog6ks6EeMC69VjkZPo=
-----END CERTIFICATE-----

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

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


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

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

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

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


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

```
  Validity End   : 02:37:09 UTC Thu Jan 15 2026
  SHA1 Fingerprint:
        209B3815271C22ADF78CB906F6A32DD9D97BBDBA


Trustpoint       : syslog-inter
================================================
CA certificate
  Serial Number  : 02:48:6A:1D:05:DC:27:34:33:79:02:BA:53:6C:27:F0:F2
  Subject:
        CN=device-syslog,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Issued By      :
        CN=Crosswork Device Root CA,O=CISCO SYSTEMS INC,L=San Jose,ST=CA,C=US
  Validity Start : 02:37:11 UTC Sat Jan 16 2021
  Validity End   : 02:37:11 UTC Mon Jan 16 2023
  SHA1 Fingerprint:
         B06F2BFDE95413A8D08A01EE3511BC3D42F01E59
RP/0/RSP0/CPU0:ASR9k(config)#logging tls-server syslog-tb131
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#tls-hostname 10.13.0.159
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#trustpoint syslog-inter
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#severity debugging
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#vrf default
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#commit
RP/0/RSP0/CPU0:ASR9k(config-logging-tls-peer)#exit
RP/0/RSP0/CPU0:ASR9k(config)#exit
RP/0/RSP0/CPU0:ASR9k#exit
RP/0/RSP0/CPU0:ASR9k#show running-config logging
Fri Jan 22 11:17:19.385 GMT
logging tls-server syslog-tb131
vrf default
severity debugging
trustpoint syslog-inter
tls-hostname <CDG Southbound IP>
!
logging trap debugging
logging format rfc5424
logging facility user
logging hostnameprefix ASR9k
logging suppress duplicates

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

Sample IOS XE device configuration to enable TLS

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

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

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

Certificate has the following attributes:
       Fingerprint MD5: D88D6D8F E53750D4 B36EB498 0A435DA1
```

```
      Fingerprint SHA1: 649DE822 1C222C1F 5101BEB8 B29CDF12 5CEE463B

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


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

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

-----BEGIN CERTIFICATE-----
MIIFfTCCA2WgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwXDELMAkGA1UEBhMCVVMx
EzARBgNVBAgMCkNhbGlmb3JuaWExDjAMBgNVBAoMBUNpc2NvMQ4wDAYDVQQLDAVT
.............................................................
.............................................................
Nmz6NQynD7bxdQa9Xq9kyPuY3ZVKXkf312IRH0MEy2yFX/tAen9JqOeZ1g8canmw
TxsWA5TLzy1RmxqQh88f0CM=
-----END CERTIFICATE-----
Trustpoint 'syslog-intermediate' is a subordinate CA.
but certificate is not a CA certificate.
Manual verification required
Certificate has the following attributes:
       Fingerprint MD5: FE27BDBE 9265208A 681670AC F59A2BF1
      Fingerprint SHA1: 03F513BD 4BEB689F A4F4E001 57EC210E 88C7BD19

csr8kv(config)#logging host <CDG Southbound IP> transport tls port 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
```

Syslog configuration to support FQDN

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

1. Configure the domain name and DNS IP 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 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 <CDG VIP FQDN>
   ```

   For IOS XE:

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

gNMI Collection Job

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

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

In gNMI, both secure and insecure modes can coexist on the device. Crosswork Network Controller gives preference to secure mode over nonsecure mode based on the information passed in the inventory.

If a device reloads, gNMI collector ensures that the existing subscriptions are resubscribed to the device.

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

Embedded Collectors support the following types of subscribe options for gNMI:

Table 14: gNMI Subscription Options

Type	Subtype	Description
Once		Collects and sends the current snapshot of the system configuration only once for all specified paths
Stream	SAMPLE	Cadence-based collection.
	ON_CHANGE	First response includes the state of all the elements for the subscribed path, followed by subsequent updates to the changed leaf values.
	TARGET_DEFINED	Router/Device chooses the mode of subscription on a per-leaf basis based on the subscribed path (i.e. one of SAMPLE or ON_CHANGE)

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

Note

- Embedded Collectors rely on the device to declare the support of one or more modes.
- gNMI sensor path with default values does not appear in the payload. This is a known protobuf behavior.

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

  Example 1:

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

  Example 2:

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

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

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

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

Enable Secure gNMI communication between Device and Crosswork

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

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

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

1. Generate the certificates. See Generate Device Certificates, on page 181.

2. Upload the certificates to the Crosswork Certificate Management UI in Cisco Crosswork. See Configure gNMI Certificate, on page 182.
3. Update device configuration with secure gNMI port details from Cisco Crosswork UI. See Update Protocol on Device from Cisco Crosswork, on page 184.
4. Enable gNMI on the device. See Device Configuration for gNMI, on page 185.
5. Enable gNMI bundling on the device. See Configuring gNMI Bundling for IOS XR, on page 186.
6. Configure the certificates and device key on the device. See Import and Install Certificates on Devices, on page 183.

Generate Device Certificates

This section explains how to create certificates with OpenSSL.

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

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

1. **Create the rootCA certificate**

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

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

2. **Create device key and certificate**

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

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

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

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

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

The following is a sample output:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            66:38:0c:59:36:59:da:8c:5f:82:3b:b8:a7:47:8f:b6:17:1f:6a:0f
        Signature Algorithm: sha256WithRSAEncryption
```

```
    Issuer: CN = rootCA
    Validity
        Not Before: Oct 28 17:44:28 2021 GMT
        Not After : Aug 17 17:44:28 2024 GMT
    Subject: CN = Crosswork
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            RSA Public-Key: (2048 bit)
            Modulus:
                00:c6:25:8a:e8:37:7f:8d:1a:7f:fa:e2:d6:10:0d:
                b8:e6:2b:b0:b0:7e:ab:c9:f9:14:a3:4f:2e:e6:30:
                97:f4:cd:d6:11:7d:c0:a6:9b:43:83:3e:26:0f:73:
                42:89:3c:d7:62:7b:04:af:0b:16:67:4c:8e:60:05:
                cc:dd:99:37:3f:a4:17:ed:ff:28:21:20:50:6f:d9:
                be:23:78:07:dc:1e:31:5e:5f:ca:54:27:e0:64:80:
                03:33:f1:cd:09:52:07:6f:13:81:1b:e1:77:e2:08:
                9f:b4:c5:97:a3:71:e8:c4:c8:60:18:fc:f3:be:5f:
                d5:37:c6:05:6e:9e:1f:65:5b:67:46:a6:d3:94:1f:
                38:36:54:be:23:28:cc:7b:a1:86:ae:bd:0d:19:1e:
                77:b7:bd:db:5a:43:1f:8b:06:4e:cd:89:88:e6:45:
                0e:e3:17:b3:0d:ba:c8:25:9f:fc:40:08:87:32:26:
                69:62:c9:57:72:8a:c2:a1:37:3f:9d:37:e9:69:33:
                a5:68:0f:8f:f4:31:a8:bc:34:93:a3:81:b9:38:87:
                2a:87:a3:4c:e0:d6:aa:ad:a7:5c:fb:98:a2:71:15:
                68:e7:8d:0f:71:9a:a1:ca:10:81:f8:f6:85:86:c1:
                06:cc:a2:47:16:89:ee:d1:90:c9:51:e1:0d:a3:2f:
                9f:0b
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Alternative Name:
            IP Address:10.58.56.18
Signature Algorithm: sha256WithRSAEncryption
     01:41:2c:91:0b:a1:10:8a:11:1a:95:36:99:2c:27:31:d3:7d:
     e9:4b:29:56:c3:b7:00:8c:f4:39:d2:8c:50:a4:da:d4:96:93:
     eb:bb:71:e3:70:d3:fe:1f:97:b2:bc:5c:f8:f4:65:ed:83:f7:
     67:56:db:0f:67:c2:3d:0c:e7:f8:37:65:1d:11:09:9a:e3:42:
     bc:c6:a0:31:7c:1f:d7:5e:c6:86:72:43:a8:c1:0c:70:33:60:
     dc:14:5b:9d:f3:ab:3d:d5:d2:94:90:1c:ba:fd:80:4d:22:e3:
     31:93:c7:16:5f:85:20:38:ad:36:b9:1a:e0:89:8e:06:8c:f8:
     cd:55:cc:a1:89:d3:91:7f:66:61:a3:40:71:c2:1e:ee:3b:80:
     37:af:73:5e:8e:0d:db:4b:49:da:a6:bd:7d:0a:aa:9e:9a:9e:
     fa:ed:05:25:08:f2:4d:cd:2f:63:55:cf:be:b1:5d:03:c2:b3:
     32:bf:f4:7b:1a:10:b9:5e:69:ac:77:5e:4a:4f:85:e3:7f:fe:
     04:df:ce:3e:bb:28:8f:e3:bf:1a:f9:0f:94:18:08:86:7d:59:
     57:71:0a:97:0d:86:9c:63:e7:0e:48:7d:f0:0e:1d:67:ff:9b:
     1d:1b:05:25:c8:c3:1f:f4:52:0f:e1:bf:86:d7:ec:47:10:bd:
     94:cf:ca:e2
```

Configure gNMI Certificate

Embedded Collectors act as the gNMI client while the device acts as the gNMI server. The collectors validate the device using a trust chain. It's expected that you have a global trust chain for all the devices. If you have multiple trust chains, add all the device trust chains (single or multiple vendors) in a single .pem file and upload this .pem file to the Crosswork Certificate Management UI.

Note You can upload only one gNMI certificate to Crosswork.

To add the gNMI certificate.

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

Step 2 Click the + icon to add the certificate.

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

- **Device Certificate Name** - Enter a name for the certificate.
- **Certificate Role** - Select **Device gNMI Communication** from the drop-down list.
- **Device Trust Chain** - Browse your local file system to the location of the rootCA file and upload it.

Step 4 Click **Save**.

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

Import and Install Certificates on Devices

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

Certificates on a Cisco IOS XR Device

To install certificates on a Cisco IOS XR device.

1. Copy rootCA.pem, device.key, and device.crt to the device under /tmp folder.
2. Log in into the IOS XR device.
3. Use the run command to enter the VM shell.

   ```
   RP/0/RP0/CPU0:xrvr-7.2.1#run
   ```
4. Navigate to the following directory:

   ```
   cd /misc/config/grpc
   ```
5. Create or replace the content of the following files:

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

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

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

Certificates on a Cisco IOS XE Device

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

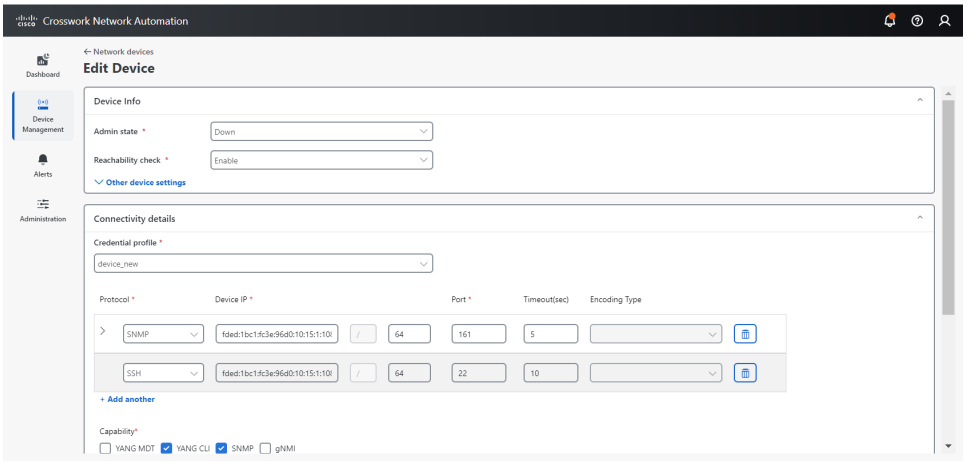
```
# Send:
Device# configure terminal
Device(config)# crypto pki import trustpoint1 pem terminal password password1

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

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

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

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

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

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

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

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

Update Protocol on Device from Cisco Crosswork

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

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

Figure 68: Edit Device Details Window



Device Configuration for gNMI

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

Cisco IOS XR devices

1. Enable gRPC over an HTTP/2 connection.

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

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

2. Set the session parameters.

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

   where:

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

- `tls-mutual`: Set the mutual authentication.
- `tls-trustpoint`: Configure trustpoint.
- `server-vrf`: Enable the server vrf.

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

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

Cisco IOS XE Devices

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

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

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

```
Device# configure terminal
Device(config)# gnmi-yang server
Device(config)# gnmi-yang secure-server
Device(config)# gnmi-yang secure-trustpoint trustpoint1
Device(config)# gnmi-yang secure-client-auth
Device(config)# gnmi-yang secure-port 50001 <The default port is 50051.>
Device(config)# end
Device
```

Configuring gNMI Bundling for IOS XR

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

Before you begin

Make sure that you are aware of the following:

- IOS XR release versions 7.81 and later support the gNMI bundling capability. For more information about how the bundling feature works, see Programmability Configuration Guide for Cisco 8000 Series Routers, IOS XR Release 7.8.x.
- The gNMI bundling capability can only be configured from the device. This option is not available in the Crosswork Interface.

Step 1 Enable the bundling feature using the following command:

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

The gNMI bundling capability is disabled by default.

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

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

The default bundling size is 32768 bytes.

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

What to do next

Verify that the bundling capability is configured using the following:

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

Create a Collection Job from Cisco Crosswork UI

Follow the steps to create a collection job:

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

Before you begin

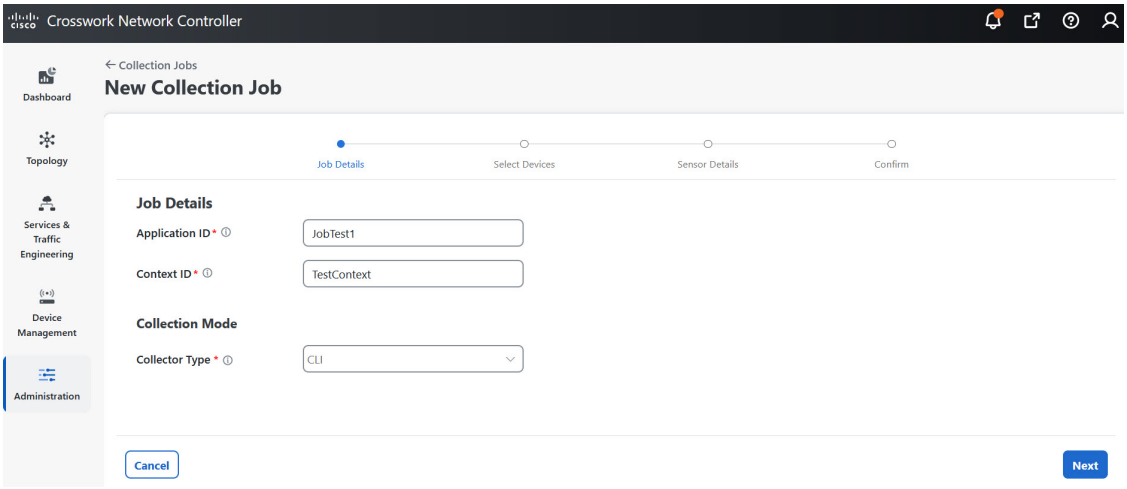
Ensure that a data destination is created (and active) to deposit the collected data. Also, have details of the sensor path and MIB that you plan to collect data from.

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

Step 2 In the left pane, click + button.

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

Figure 69: Job Details Window

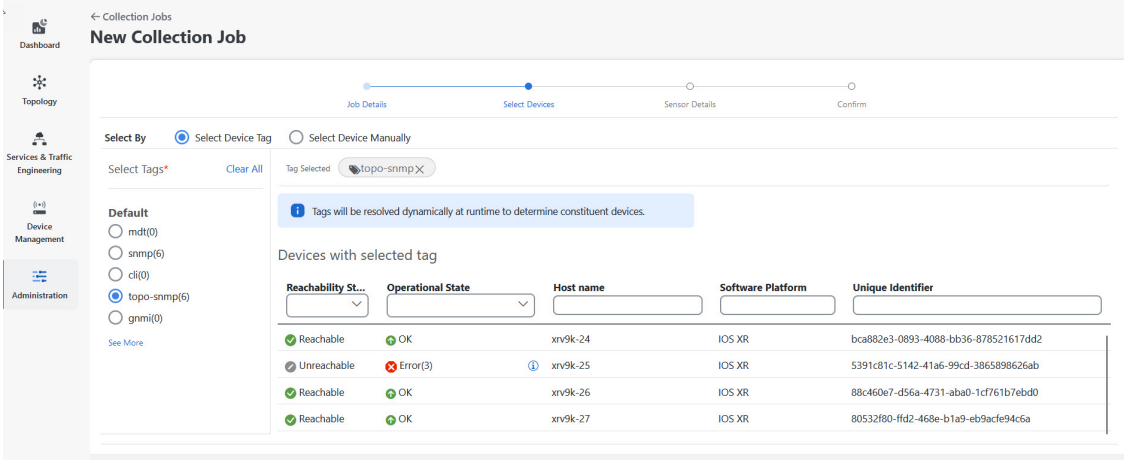


- Application ID: A unique identifier for the application.
- Context: A unique identifier to identify your application subscription across all collection jobs.
- Collector Type: Select the type of collection - CLI or SNMP.

Click **Next**.

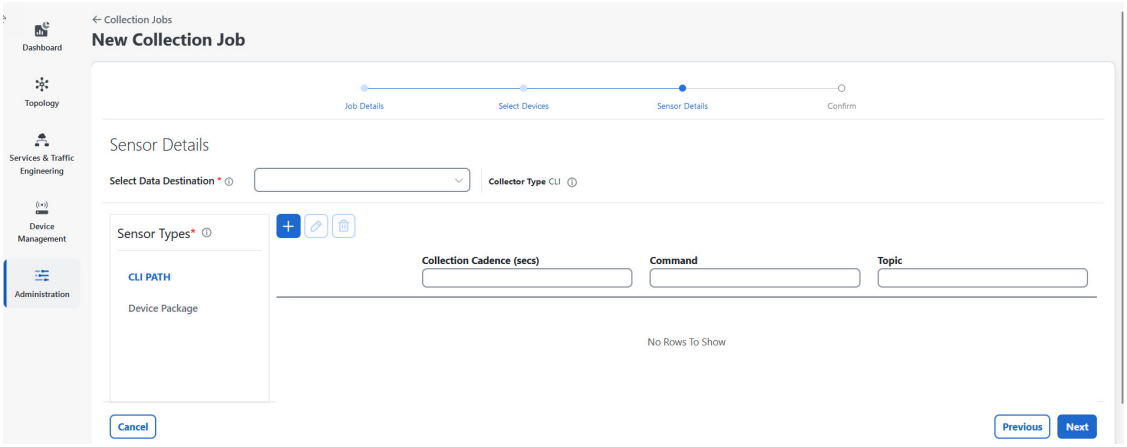
Step 4 Select the devices from which the data is to be collected. You can either select based on device tag or manually. Click **Next**.

Figure 70: Select Devices Window



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

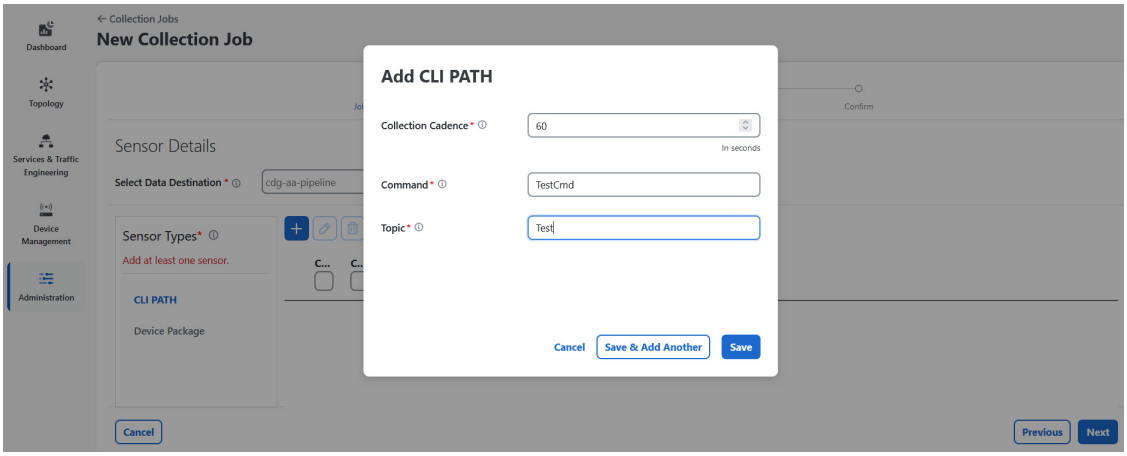
Figure 71: Sensor Details Window for CLI Path



- Select data destination from the **Select Data Destination** drop-down list.
- Select sensor type from **Sensor Types** pane on the left.

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

Figure 72: Add CLI Path Dialog Box

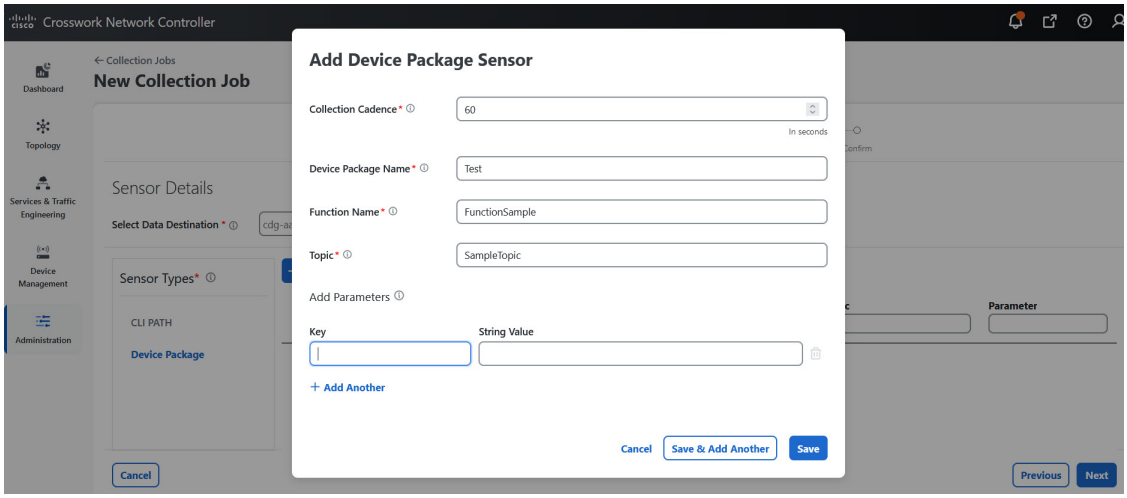


- Collection Cadence: Push or poll cadence in seconds.
- Command: CLI command
- Topic: Topic associated with the output destination.

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

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

Figure 73: Add Device Package Sensor Dialog Box



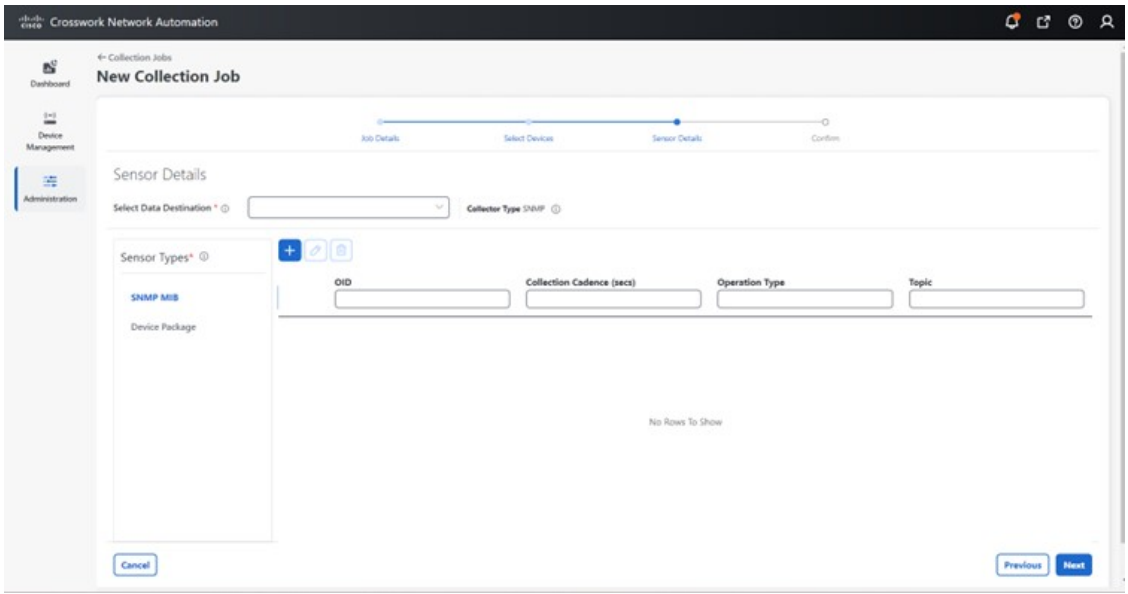
- Collection cadence: Push or poll cadence in seconds.
- Device Package Name: Custom XDE device package ID used while creating device package.
- Function name: Function name within custom XDE device package.
- Topic: Topic associated with the output destination.

Enter Key and String value for the paramters.

Click **Save**.

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

Figure 74: Sensor Details Window for SNMP Path

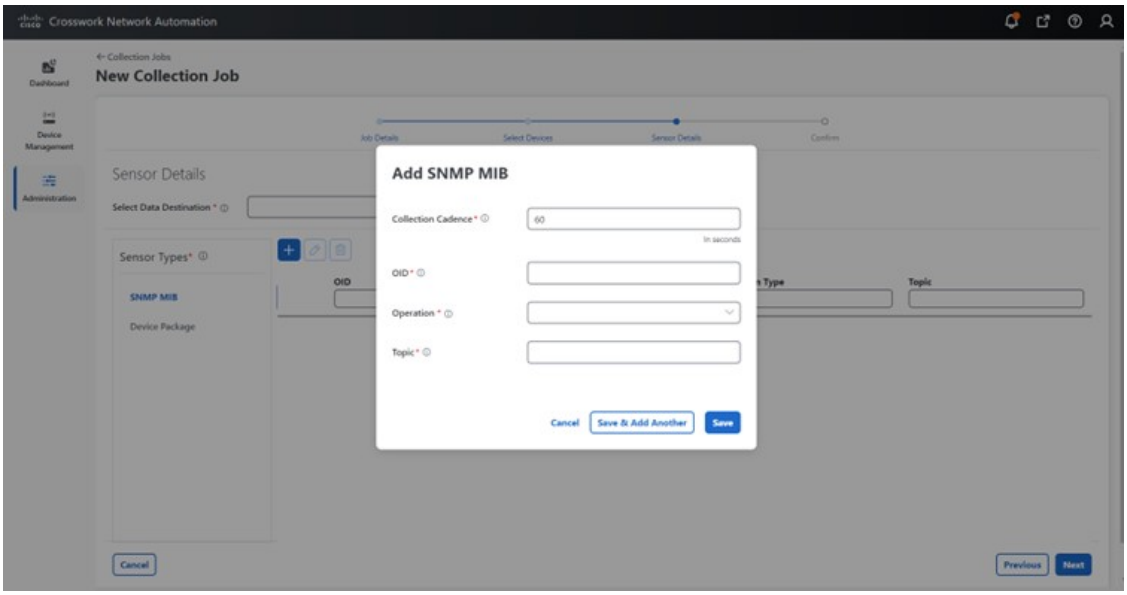


- Select data destination from the **Select Data Destination** drop-down list.

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

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

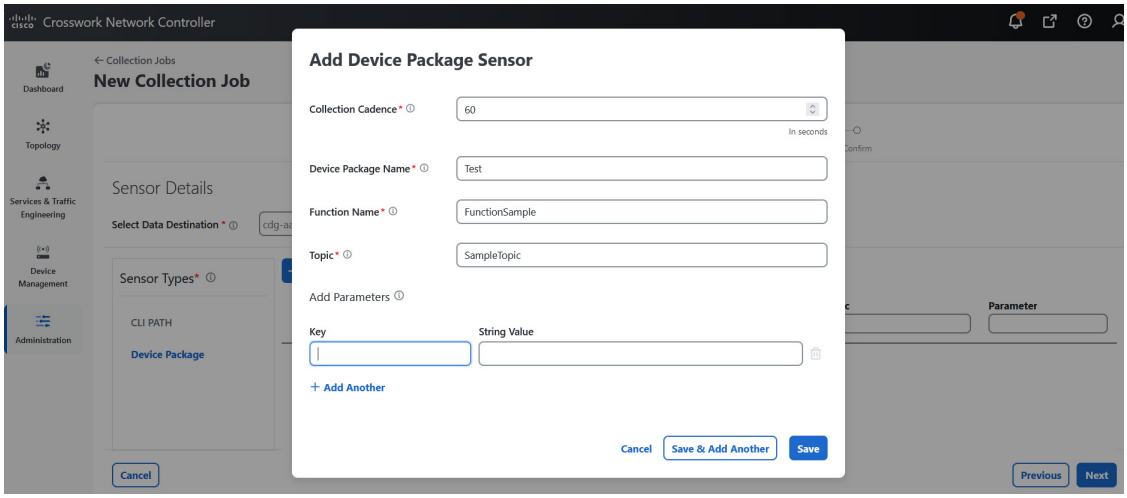
Figure 75: Add SNMP MIB Dialog Box



- Collection Cadence: Push or poll cadence in seconds.
- OID
- Operation: Select the operation from the list.
- Topic: Topic associated with the output destination.

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

Figure 76: Add Device Package Sensor Dialog Box



- Collection Cadence: Push or poll cadence in seconds.
- Device Package Name: Custom device package ID used while creating device package.
- Function name: Function name within custom device package.
- Topic: Topic associated with the output destination.

Enter Key and String value for the parameters.

Click **Save**.

Step 7 Click **Create Collection Job**.

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

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

```
netstat -tulpn
```

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

Monitor Collection Jobs

You can monitor the status of the collection jobs currently active on all Embedded Collectors instances that are enrolled with Crosswork Network Controller from the **Collection Jobs** page.

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

This left pane lists all active collection jobs along with their Status, App ID, Context ID, and Action. The Action drop-down lets you:

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

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.

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

- Application name and context that is associated with the collection job.
- Status of the collection job.

Note

- The status of a collection task associated with a device after it is attached to 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.

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

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

Crosswork Network Controller also displays the following details for collections and distributions:

Field	Description
Collection/Distribution Status	Status of the collection/distribution. It is reported on a on change basis from Embedded Collectors. Click next to the collection/distribution status for details.
Hostname	Device hostname with which the collection job is associated.
Device Id	Unique identifier of the device from which data is being collected.
Sensor Data	Sensor path Click to see collection/distribution summary. From the sensor data summary pop-up you can copy the sensor data by clicking **Copy to Clipboard**. Click to see collection/distribution metrics summary. The metrics are reported on 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 on which the last status change was reported for that device sensor pair from Embedded Collectors.

Note

- `Create Failed` error means out of N devices, some devices failed to set up. However, the collection would happen on the devices that were successfully set up. You can identify one or more devices causing this error by using the `Control Status` API.
- If job creation failed on a particular device because of NSO errors, after fixing NSO errors, you have to manually change the administration state of the device first to "Down" and then "Up". However, doing so resets the collection on the device.

Note

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

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

Collection Status for Event-Based Collection Jobs

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

Delete a Collection Job

System jobs (default jobs created by various Crosswork Applications) should not be deleted as it causes collection issues. Jobs created by Health Insights should only be deleted by disabling the KPI profile which will remove the collection jobs it deployed. When you delete a collection job, it deletes the associated collection tasks.

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

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

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

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

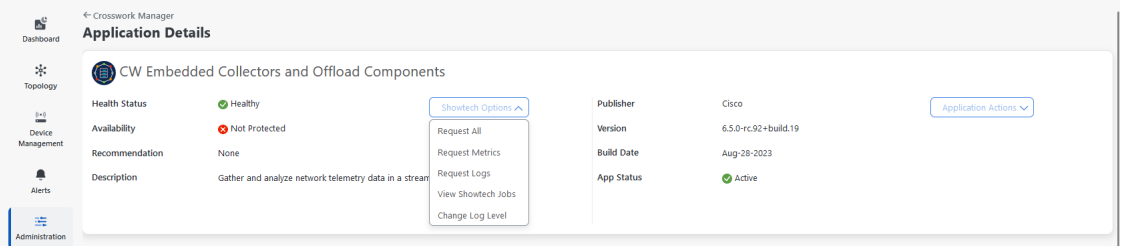
Step 4 In the corresponding row, click ... and select **Delete**. The **Delete Collection Job** window is displayed.

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

Monitor Embedded Collectors Application Health

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 Embedded Collectors application's overall health is influenced by the health of each individual pod service.

Figure 77: Crosswork Embedded Collector and Offload Component Pane



To review the collector health status, navigate to the Crosswork UI:

Step 1 From the main menu, choose **Administration > Crosswork Manager > CW Embedded Collectors and Offload Components** tile.

Step 2 (Optional) From the **Showtech Options** drop-down, you can perform the following operations:

- **Request All**: Collects both logs and metrics. To view the logs, navigate to **Crosswork Manager > Application Management > Showtech Requests** to view the logs.
- **Request Metrics**: Collects the metrics information.
- **Request Logs**: Collects the log information.
- **View Showtech Jobs**: Displays the progress of the Showtech jobs. Alternatively, you can also see the job's status and other details from **Crosswork Manager > Application Management > Showtech Requests**.
- **Change Log Level**: Enables you to change the log level of various components within the embedded collector, such as collectors (cli-collector) and infrastructure services (oam-manager). Log level changes only impact the collector where the change is being made.

Step 3 (Optional) From the **Application Actions** drop-down, you can perform the following operations:

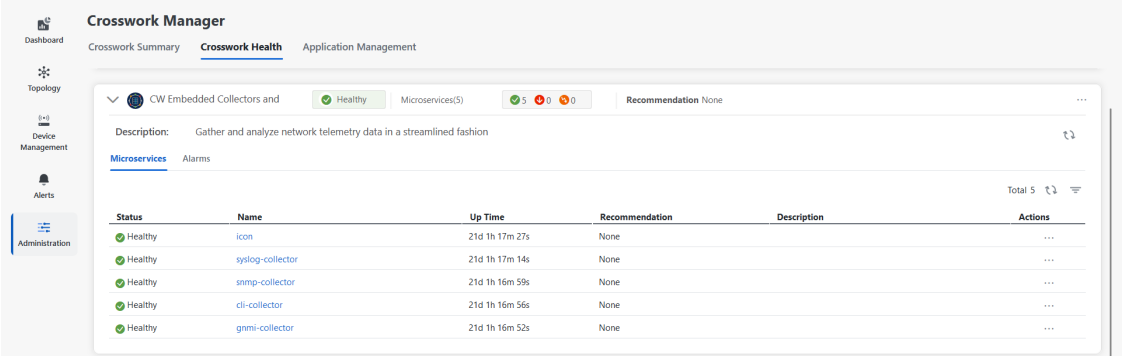
- **Install**: Installs new collector with the same information (profile, hostname, management interface) as the previous collectors.
- **Upgrade**: Upgrades the collector version.
- **Activate**: Activate the collectors.

- **Uninstall**: Removes the collector app. The execution of this operation has consequences for the collection jobs currently in progress.

Monitor the Collector's Pod Health

In the Embedded Collector and Offload Component pane, you can get a detailed overview of the health status of the pods that host the collectors or microservices. We suggest regularly monitoring the health of the collector pods in your network to avoid overloading and taking proactive corrective measures, such as adding more resources or reducing the load on the collector in a timely manner.

Figure 78: Microservices Tab



To view the pod health status, navigate to the Crosswork UI:

Step 1 From the main menu, choose **Administration > Crosswork Manager > CW Embedded Collectors and Offload Components**.

Step 2 Expand the **CW Embedded Collectors and Offload Components** pane and the click the **Microservices** tab.

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 the following actions:

- **Restart**– Restarts the collector pod. Restarting a pod causes disruption in the ongoing collection process. Whenever you need to restart, start, or stop a process, we strongly advise to consult the Cisco TAC team.
- **Showtech Requests**– Displays the showtech jobs executed for the corresponding collector pod. You have to navigate to **Crosswork Manager > Application Management > Showtech Requests** to view the logs.
- **Request All**– Collects both logs and metrics of the pod. To view the logs, navigate to **Crosswork Manager > Application Management > Showtech Requests** to view the logs.
- **Request Metrics**– Collects the metrics of the pod.
- **Request Logs**– Collects the logs of the pod.

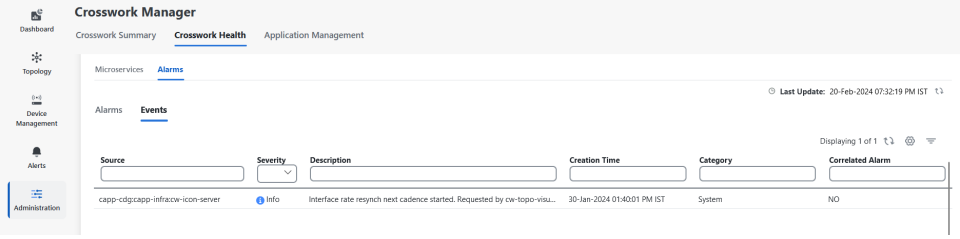
Viewing Collector Alarms and Events

Embedded Collectors generate an alarm when it detects an anomaly that prevents data collections. Monitoring the alarms enables you to detect the potential collector issues affecting data collection, and take the remediation action, if necessary.

To view the alarms, from the Crosswork Network Controller UI, choose **Administration > Crosswork Manager > CW Embedded Collectors and Offload Components**.

The **Alarms** tab provides a consolidated list of all collector alerts and events. You can toggle between the **Alarms** and **Events** subtabs to view the respective details.

Figure 79: Events Tab



Filter the list of alarms or events by filtering columns, changing the **Active Alarms Only** slider, or adding or removing columns using the icon.

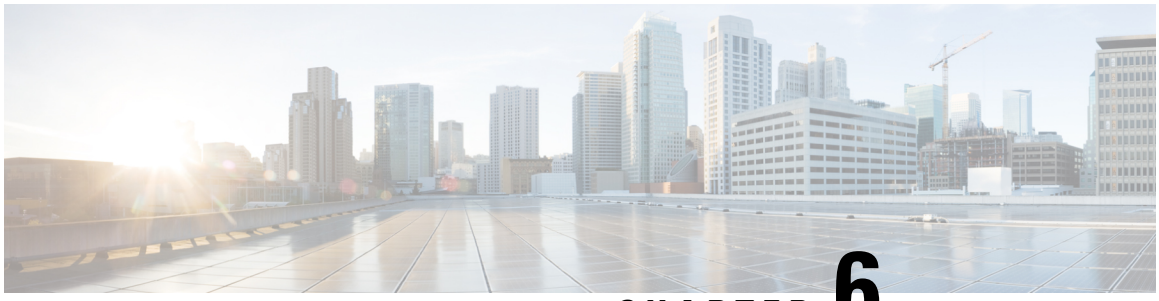
Troubleshoot Embedded Collectors

The troubleshooting section contains information about the possible issues and corrective actions that you may observe with Embedded Collectors.

Admin State Automatically Changes from DOWN to UP

In a single VM deployment, the devices are automatically attached to Embedded Collectors, and their Admin State is changed from DOWN to UP.

Workaround: If you want to change the state to DOWN, manually change it through the **Edit Device** page. For more information about editing a device, see *Edit Devices* section in the *Cisco Crosswork Network Controller 7.0 Device Lifecycle Management*.



CHAPTER 6

Set Up and Use Your Topology Map for Network Visualization

Overview of the Topology Map

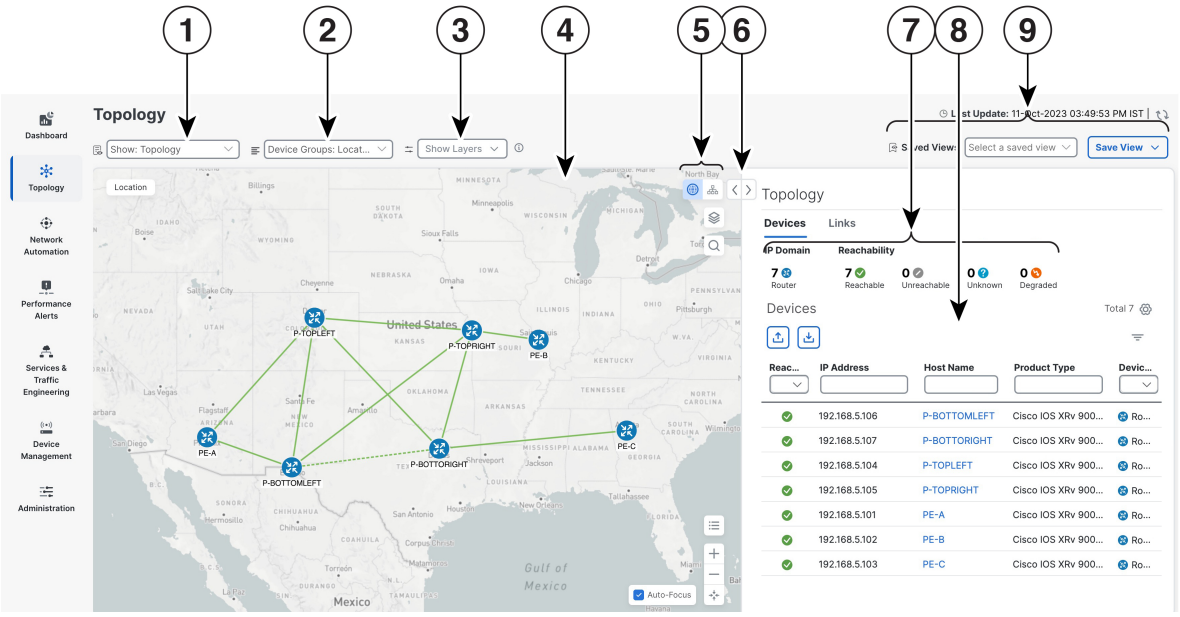
You can view the network devices and their connections in different ways on the topology map.

You can choose between a logical map or a geographical map, depending on your preference. The logical map arranges the devices and links based on an algorithm that you can modify, without considering their physical location. The geographical map places the devices, clusters, links, and tunnels on a world map, using the GPS coordinates of each device from the device inventory.

To use the topology map, you have to onboard the devices on the system first, for more information refer to Add Devices to the Inventory, on page 275.

You can also filter your topology view by creating device groups. For more information, refer to Use Device Groups to Filter your Topology Map, on page 205.

Figure 80: Topology Home page



Callout No.	Description
1	**Topology Map View**: From the **Show** drop-down list, click the option that displays the data that you would like to see on the map. You can view the following options. • Topology • Traffic Engineering • VPN Services • Transport Slicing
2	**Device Groups**: From the drop-down list, click the group of devices you want to display on the map. All other devices will be hidden.
3	**Show Layers**: From the drop-down list, click the network layers you want displayed on the map. All devices and links that belong to the selected layers are then displayed. By default, all layers are displayed.

Callout No.	Description

4	**Topology Map**: The topology map can be displayed on a logical map or a geographical map, where the devices and links are shown in their geographic context. From the map, you can drill down to get detailed information about devices and links.
	
	Devices:
	
	• To view basic device information, hover the mouse pointer over the device icon. A pop up window displaying the host name, state, node IP, and device type appears.
	
	• To view device details, click on the device icon. For more information see, View Basic Device Details, on page 208
	
	If you have installed Element Management Functions:
	
	• The following additional information will be displayed in the **Device Details** screen.
	
	  • Alarm information under Summary in the **Details** tab.
	
	  • **Interface** tab with name, and operational and admin status for each associated interface.
	
	  • 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, oper 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.
	
	  Note Relevant performance policies should be created to see the history for a specific device or link.
	
	Links:
	
	• A solid line represents a *single link* between two devices. A dashed line represents an *aggregated* link, which could indicate multiple links, such as several Layer 2 links (two Ethernet links for example) or several Layer 3 links (2 ISIS links) on the same physical link. To configure the dashed link, refer to Differentiate Aggregated Links from Single Links, on page 221.
	
	  For easy identification, you can color links on the map based on criteria such as link down and utilization. For more information, refer to Differentiate all Down Links, on page 222 and Show Link Health by Color, on page 223.
	
	• A and Z indicates connecting interfaces.
	
	• To view link information details, click on the link, and the **Links** panel is displayed on the right-hand side with information.

Callout No.	Description
5	 : The logical map shows devices and their links, positioned according to an automatic layout algorithm, ignoring their geographical location. You can change the layout algorithm.  : The geographical map shows single devices, device clusters, and links, superimposed on a map of the world. Each device location on the map reflects the device's GPS coordinates (longitude and latitude) as defined in the device inventory.  : The Display Preferences window allows you to change display settings for devices, links. You can also change the display preferences for the alarms by enabling alarm visualization using the **Show Alarms** option in the **Alarms** tab and set a severity filter to show only the alarms of the selected severity or higher. Once enabled, the alarm notification icon will be displayed on the devices in the topology map in case of an alarm. **Note** Settings changes only apply to the current session and will revert to the defaults when you log out and log in again. To retain your changes for future use, save your view before logging out.  : The global search allows you to search the topology using device names, location or the device civic location.
6	**Expand/Collapse/Hide Side Panel**: Expand or collapse the contents of the side panel. Close the side panel to get a larger view of the topology map.
7	The **Mini Dashboard** provides a summary of the IP Domain and device reachability status. If filters are applied, the **Mini Dashboard** is updated to reflect what is displayed in the Devices table. **Note** If you have installed Element Management Functions, the **Alarm Severity** information is displayed in the Mini Dashboard and a **Severity** column is added to the Devices table. You can refine the table based on the severity value.
8	The content of this window changes depending on what applications you have installed, what **Show** is set to for the topology map and if you have selected to view more information on the device.
9	**Saved Views**: Lets you create a named custom view using the settings and layout for your current map, settings of the tables saved in the saved views, or display a custom view you have created previously.

Use Internal Maps Offline for Geographical Map Display

The system is set up by default to get the geo map tiles from a specific Mapbox URL through a direct Internet connection. If you do not have an Internet connection and therefore the system cannot access an external map provider to retrieve geographical map tiles, you can upload internal map files to represent the areas of the world you require for your network. These map files must be downloaded from Cisco.com and then uploaded into the system. The name of the map file indicates the area of the world it contains, for example,

africa-geomaps-1.0.0-for-Crosswork-x.x-signed.tar.gz. If you will be managing a network in a specific part of the world, upload only the relevant map files. You do not need to upload all available map files.

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.

To use internal maps to display the geographical map:

Before you begin

Download the required map files from Cisco.com and place them on an accessible server. The server must support SCP protocol for file transfer.

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings**.

Step 2 Under **Topology**, click the **Map** option.

Step 3 Select the **Work offline with internal maps** radio button and click **Manage**.

Step 4 In the Manage Internal Maps dialog, click to upload a new map file. Note that you can upload one file at a time.

Step 5 In the Upload Map File dialog, browse to the location of the map file you downloaded so that the system can access the file.

Step 6 Click **Upload**.
The system uploads the map from the specified location. The upload process might take some time and must not be interrupted by closing the browser or clicking Cancel. When the process is complete, the new map appears under **Uploaded Maps** in the Manage Internal Maps dialog.

Step 7 Upload additional maps, as required.

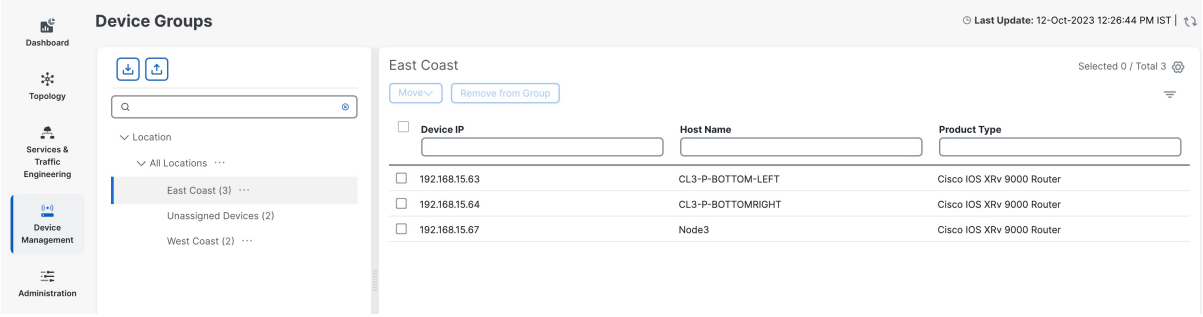
Use Device Groups to Filter your Topology Map

Device groups let you organize and manage your devices according to your needs. You can use device groups to filter and display data from specific devices on your dashboard. Device groups also allow you to visualize and zoom in on data specific to a particular group of devices. It reduces the clutter on your screen and allows you to focus on data that is most important to you.

Create Device Groups

You can create device groups and add devices to the groups either manually (as described in this section) or automatically, as described in Create Rules for Dynamic Device Grouping, on page 206. A device can belong to only one device group.

Figure 81: Device Groups



Step 1 From the main menu choose **Device Management** > **Device Groups**. We see that the East Coast device group has been selected. Also note that only the devices belonging to the East Coast device group are listed in the devices table in the right pane.

Step 2 To add a new sub-group, click the three dots next to any group and then click **Add a Sub-group**.

Step 3 Fill in the details and click **Create**.
A new sub-group is added under the selected parent group.

Create Rules for Dynamic Device Grouping

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. Any newly added or discovered devices that match the rule will be placed in the appropriate group.

Dynamic rules do not apply to devices that already belong to groups. You must move them to Unassigned Devices if you want them to be considered by the rule.

Before you begin

While you can follow examples given in the Dynamic Groups dialog, it is helpful to be familiar with Regular Expressions.

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, click **Test Rule** to view a sampling of what type of group names will be created.

Step 5 Turn the **Enable Rule** toggle ON to enable the rule. After the rule is enabled, the system checks for unassigned devices every minute and will assign them to the appropriate group based on the rule.

Step 6 Click **Save**.

Step 7 Groups that are created this way initially appear under Unassigned Groups (created when a rule is enabled for the first time). Move newly created groups to the desired group hierarchy.

Modify Device Groups

You can modify device groups to add or edit the device group details. You can change the group name, or assign a different parent group.

Step 1 From the main menu choose **Device Management** > **Device Groups**.

Step 2 To edit the group details, click the three dots next to the group name and then click **Edit Group Properties**. You can update the parent group, group name and the description.

Step 3 Click **Save**.

Delete Device Groups

You can delete a device groups from the system. This will unassign all the devices that belong to that group and make them available for other groups.

Step 1 From the main menu choose **Device Management** > **Device Groups**.

Step 2 To delete the device group, click the three dots next to the group name and then click **Delete Group**.

Step 3 On the **Delete Group** pop-up, click **Delete** to confirm your deletion.

Move Devices from One Group to Another

If you need to reorganize your devices, you can move them from one group to another.

Step 1 From the main menu choose **Device Management** > **Device Groups**.

Step 2 Select the group from which you wish to move the devices.

Step 3 Select the devices from the right pane.

Step 4 From the **Move** drop-down, select the appropriate group and click **Move**. You can also create a new group to which you can move your selected devices. For more information refer to Create Device Groups, on page 205

Import Multiple Device Groups

When you import device groups from a CSV file, the import process creates new device groups that does not exist in the database, and updates the existing device groups that have the same data as the imported ones. This means that you might lose some of your original data if you import device groups without backing them up first. Therefore, we recommend that you export a copy of all your current device groups before you perform an import.

Step 1 From the main menu, choose **Device Management** > **Device Groups**.

Step 2 Click to open the **Import Groups** dialog box.

Step 3 If you have not already created a device groups CSV file to import:

a) Click the **Download device groups (*.csv)' template** 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 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.

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.

c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

Step 5 With the CSV file selected, click **Import**.

Note
- While importing device groups using a CSV file, you should wait for the operation to complete. Clicking the **Import** button while the operation is in progress will lead to duplicate entries.

Export Multiple Device Groups

You can export the device groups details to a CSV file. This is useful for creating a record of all the device groups in the system at a given time. You can also modify the CSV file as you wish, and import it back to update the existing data.

Step 1 From the main menu, choose **Device Management** > **Device Groups**.

Step 2 Click to export the device groups in CSV format. The CSV file is then downloaded in your systems download folder.

View Device Details from the Topology Map

The topology map lets you view the information of any device in your network. You can see various details, such as device specifications, routing configurations, and device links. The topology map enables you to monitor and manage your network devices with ease and efficiency.

View Basic Device Details

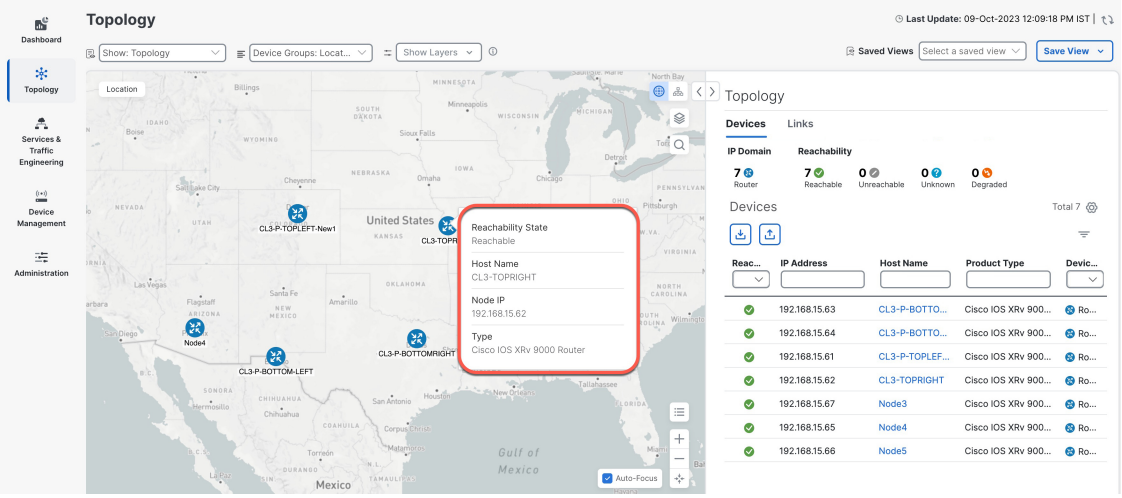
You can view the basic device details and its connections in a graphical way. The map also allows you to adjust the view of the device by zooming in and out, panning, and rotating.

Note If you are viewing the HTML version of this guide, click on the images to view them in full-size.

Step 1 From the main menu choose **Topology**.

Step 2 Hover the mouse over the device icon, to quickly view the host name, reachability state, IP address and type of device.

Figure 82: Basic Device Details



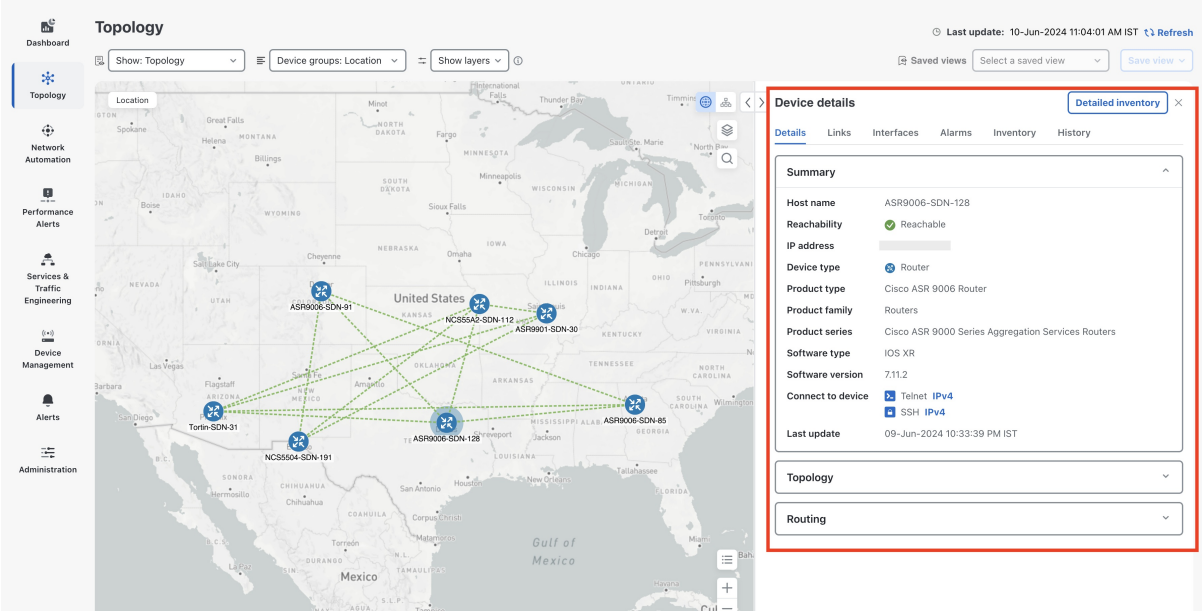
View All Device Details

The device icon on your topology map lets you view more details about your device, such as where it is located, what kind of device it is, when it was last updated and more.

Step 1 From the main menu choose **Topology**.

Step 2 To view device details, click on the device icon. The following details are displayed.

Figure 83: Device Details



If you have installed Element Management Functions, the following additional information will be 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.

Identify Device Routing Details

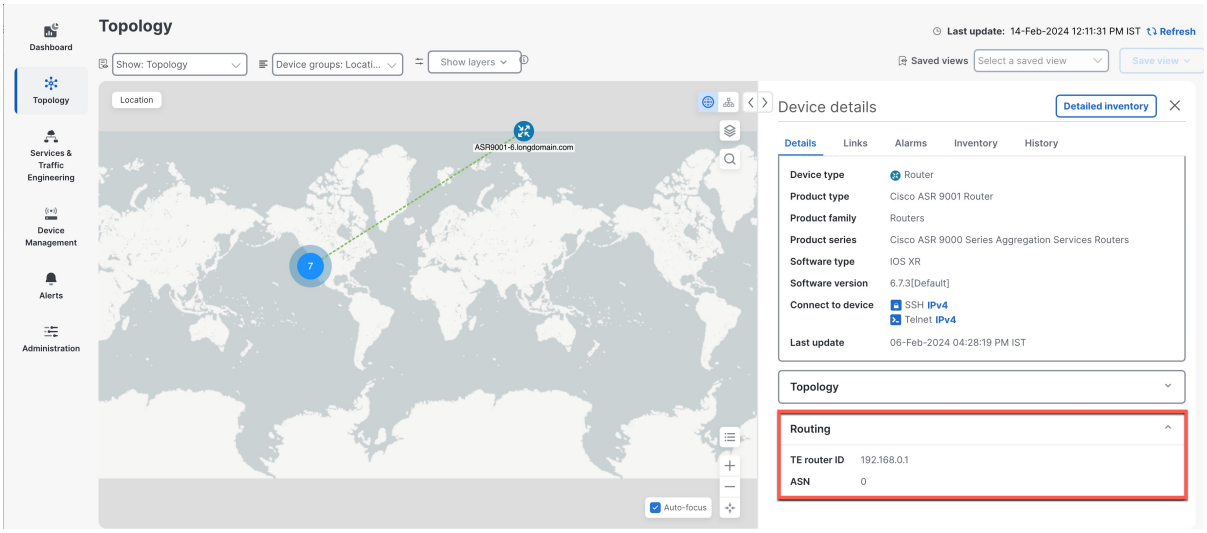
Device routing determines how data packets are transmitted from one device to another in the network and ensures that data packets reach their intended destination, avoiding congestion or loops in the network.

Note If you are viewing the HTML version of this guide, click on the images to view them in full-size.

Step 1 From the main menu choose **Topology**.

Step 2 To view the device routing details, on the topology map, click the device icon. You can view the routing details in the right pane.

Figure 84: Device Routing Details



Identify the Links on a Device

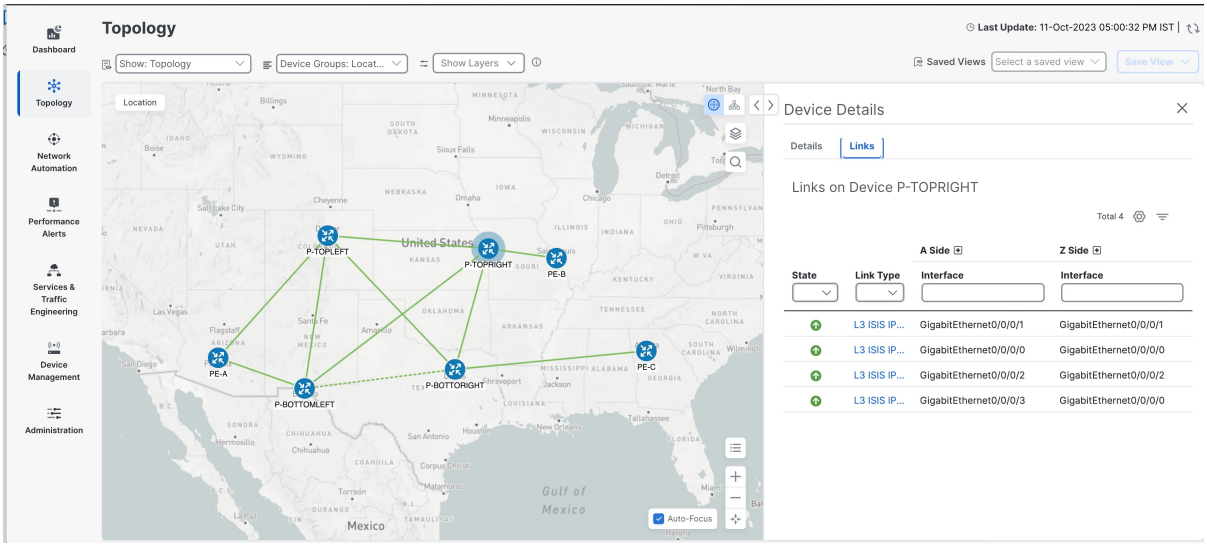
You can see which links are connected to the device in the Links tab in the Device Details pane.

Step 1 From the main menu choose **Topology**.

Step 2 To view links on the device, click on the device icon.

Step 3 In the right pane, click the **Links** tab and expand the right panel to view all the link details.

Figure 85: Links on a Device



Get Details About Topology Links

You can view detailed information about any link on the topology map, such as the link name, source and destination devices, link status, bandwidth, latency, and link details. You can also view link utilization to see how much bandwidth the link is using, as well as packet drops and traffic volume.

View Link Details

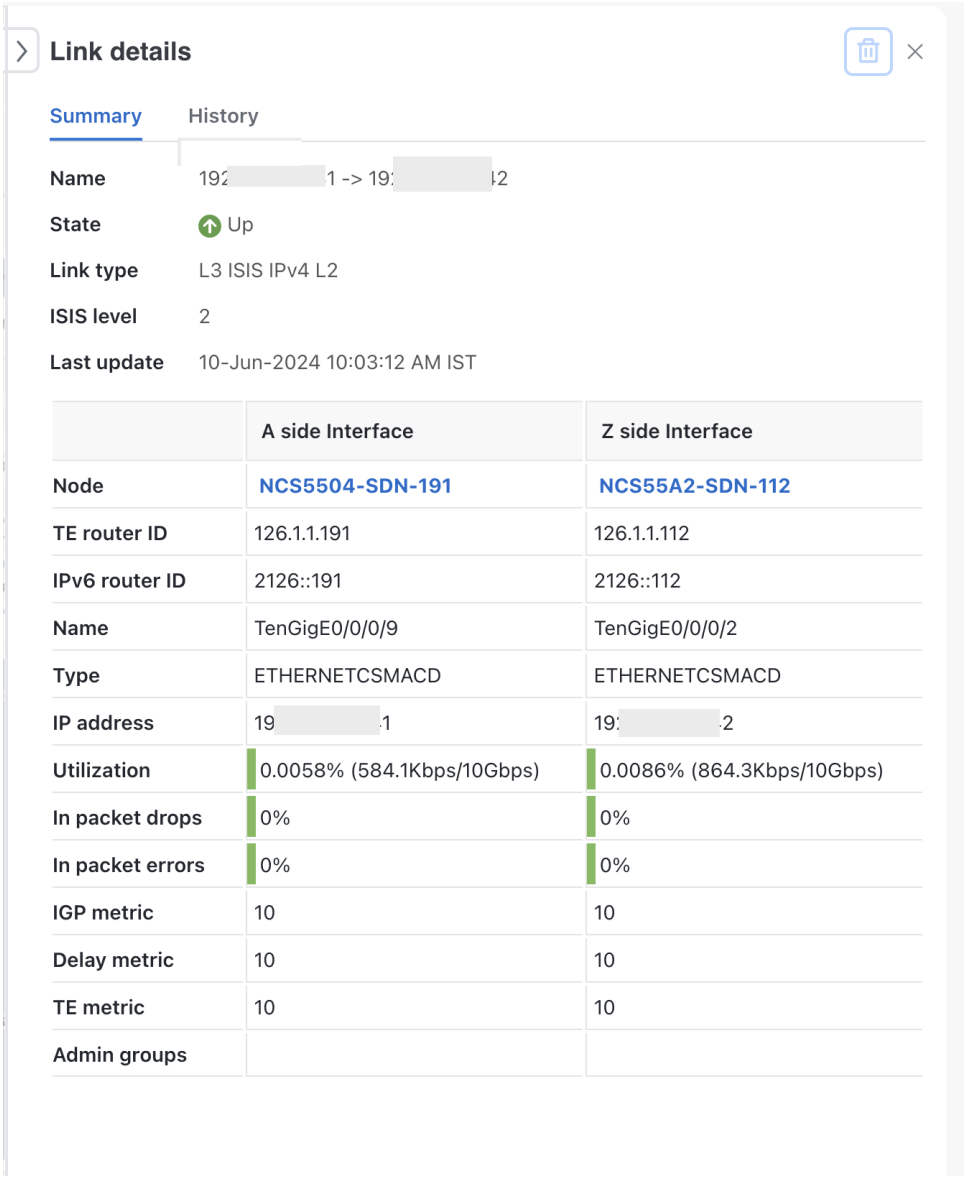
You can view the link details such as name, state, type, and endpoint interface information for each link. For more information on the link state, refer to Link States and Discovery Methods, on page 215

Step 1 From the main menu choose **Topology**.

Step 2 Select a link to view details in any of the following ways:

- By clicking a link on the topology map
- By clicking a link from the **Links** tab in the topology map
- By clicking a link from the **Links** tab in the **Device Details** page.

Figure 86: Link Details



The **History** tab provides useful insights into the performance and trends of the network. You can select the time interval to analyze the data.

Note Delay and jitter metrics are available only when Segment Routing Performance Monitoring (SR-PM) is enabled. This requires installing Service Health, which 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 7.0 Service Health Monitoring guide.

Step 3 View aggregate link details.

Click on a dashed line in the topology map. A dashed line indicates an aggregated link that represents more than one link.

Step 4 View IPv4 unnumbered interface information (if available).

IPv4 unnumbered interfaces information is displayed as a combination of the TE Router ID and the index.

View Link Interface Metrics

Link interface metrics are a set of indicators that measure the performance and quality of the communication between two or more network devices. They include parameters such as bandwidth, delay, jitter, packet loss.

Note Delay and jitter metrics are available only when Segment Routing Performance Monitoring (SR-PM) is enabled. This requires installing Service Health, which 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 7.0 Service Health Monitoring guide.

Link interface metrics can help network administrators to monitor and troubleshoot network issues, optimize network resources, and plan for future network expansion or upgrade.

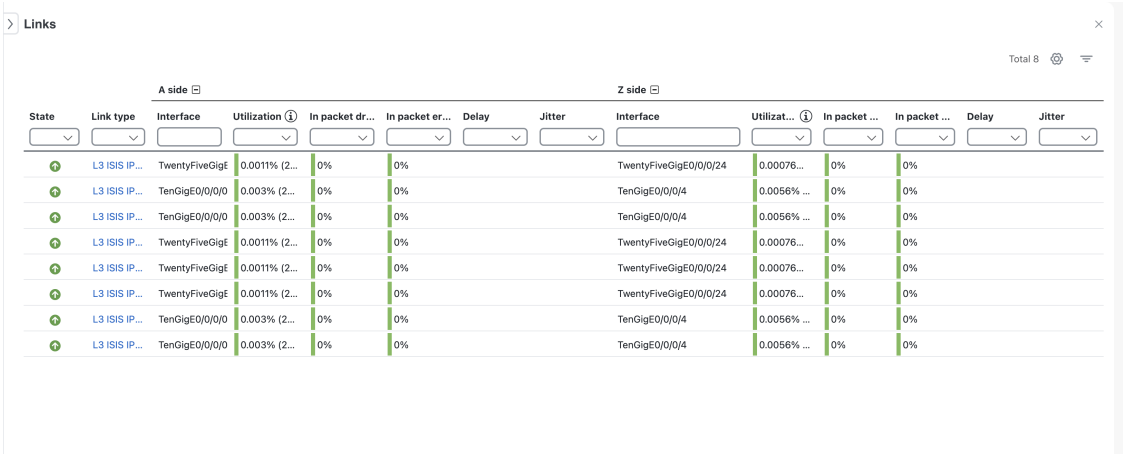
Step 1 From the main menu choose **Topology**.

Step 2 Click a link on the topology map.

Step 3 To view interface metrics, expand **A side** or **Z side**.

The utilization shown on IPv4 and IPv6 links represents the aggregate traffic and packet drops on the interface, not specific to each address family. Sub-interfaces will not show a utilization since they do not have a bandwidth like a physical interface. Traffic measurements will still be collected and displayed.

Figure 87: Link Interface Metrics



Link States and Discovery Methods

Table 15: Link Types, Discovery and States

Link Type	Discovery	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
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.

Protocols Used for Topology Services

The following table lists the protocols and methods used for obtaining the topology information.

Protocol/Method	Provides	Use Cases
IGP/ BGP-LS (via SR-PCE)	Real time topology (nodes, links, link metrics, and so on.)	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
SNMP (SNMPv2-MIB, IP-MIB, IF-MIB, LLDP-MIB, (CISCO CDB-MIB) (via CDG)	System info, interface table (interface and SR-TE/RSVP-TE traffic Utilization) IP address table, L2 adjacency information	Device management and details and Crosswork Optimization Engine model building: • 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.	To match the DLM node with the same TE router ID that is learned from the SR-PCE

Enable or Disable Topology Link Discovery

To control the visibility of L2 topology links on the maps, you can change the system settings for the discovery of LLDP, CDP and LAG protocols. These protocols are used to identify the neighboring devices and their connections. The discovery option is disabled by default, which means the links of these protocols, including the ones that were already discovered, will not show up on the maps. You can enable the discovery option to see the links of the selected protocols on the maps.

To enable topology discovery:

Before you begin

- Make sure all pods are healthy before changing the settings.

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings**.

Step 2 Under **Topology**, click the **Discovery** option.

Step 3 Select the checkbox of the protocols for which you want to enable discovery.

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

When you enable discovery, the collection jobs will be created. The table below lists the collections jobs created for each protocol setting along with the sensor paths.

Table 16: 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** `IF-MIB` is required, but it is collected in the ICON jobs.	`IP - MIB : IP-MIB / ipAddressTable / ipAddressEntry` `IF-MIB:notifications`
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`

L2 Configuration Setting	Helios collection Jobs ID	Context ID	MIBs collected	Sensor paths
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

The table below lists the common errors when enabling or disabling topology discovery:

Table 17: Common error scenarios:

Possible Error Scenario	Cause	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.

Possible Error Scenario	Cause	Cause Recommended Action
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 and Export Geographical Data

Using Keyhole Markup Language (KML) files, you can import and export the geographic location identifiers for your devices. KML is a format that encodes and stores geographic information for display on a map.

Import Geographical Data to Keynote Markup Language (KML) Format

You can import a KML file containing geographic location identifiers for multiple devices so that they can be displayed on within their geographic context on the topology map. To import a KML file into your application, follow these steps:

Step 1 From the main menu, choose **Topology**.

Step 2 Click  to open the **Import KML File** dialog box.

Step 3 If you have not already created a device KML file to import:

a) Click the **Download KML file (*.kml)' template** link and save the KML 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) When you are finished, save the new KML file.

Step 4 Click **Browse** to navigate to the file you just created and then click **Open** to select it.

Step 5 With the KML file selected, click **Import**.

Note While importing the details via UI using a KML file, you should wait for the operation to complete. Clicking the **Import** button while the operation is in progress will lead to duplicate entries for each device or provider.

Export Geographical Data to Keyhole Markup Language (KML) Format

You can export geographic location identifiers for your devices to a KML file. You can use the exported data in other contexts, if required. To export a KML file, follow these steps:

Step 1 From the main menu, choose **Topology**.

Step 2 In the right pane, click the to export the geographical data to a KML file. The KML file is downloaded to your system's download folder.

Customize your Map for your Needs

You can configure various visual settings in order to customize the map display for your requirements.

Show or Hide Device State

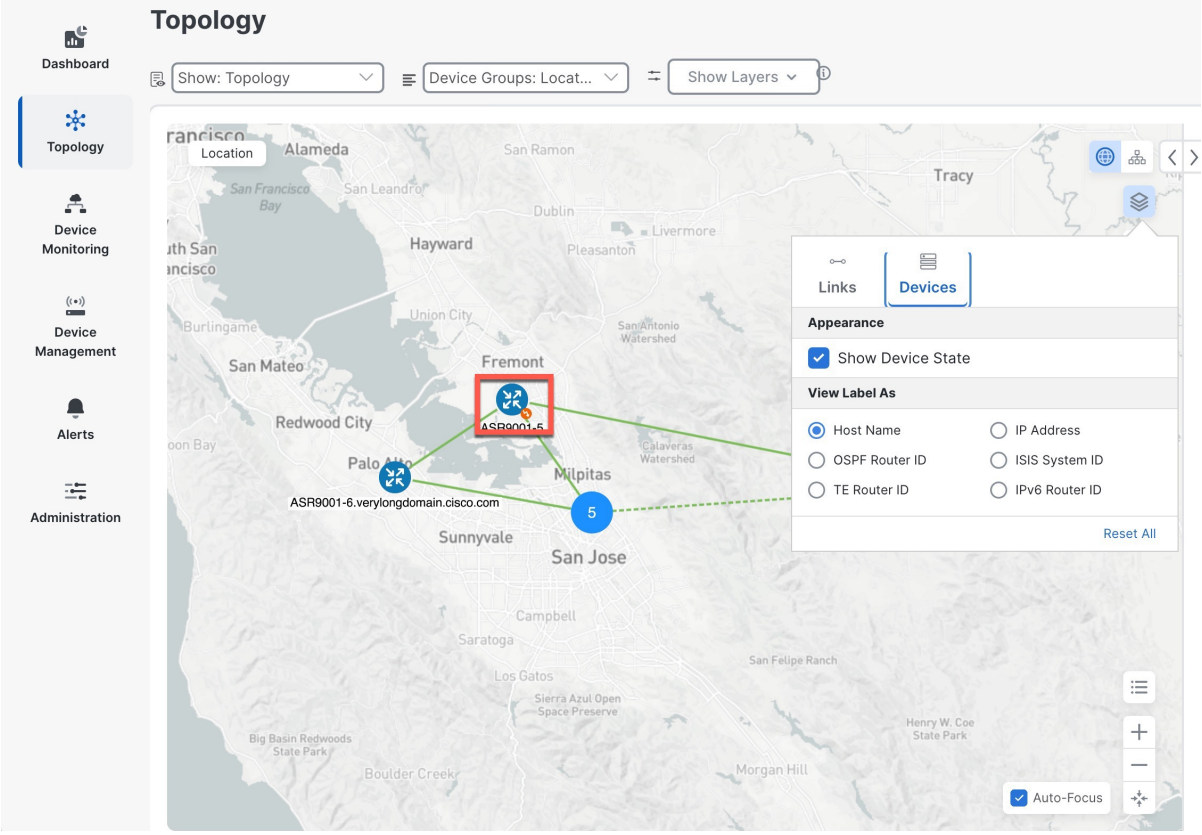
This option allows you to decide whether or not to show the device state on the topology map. You can choose to show or hide the device state according to your preference.

Step 1 From the main menu click **Topology**.

Step 2 Click on the topology map to open the **Display Preference** dialog box.

Step 3 Click the **Devices** tab and check the **Show Device State** checkbox. By default the Device State is enabled and is shown on the map.

Figure 88: Show or Hide Device State



Define the Device Label Type

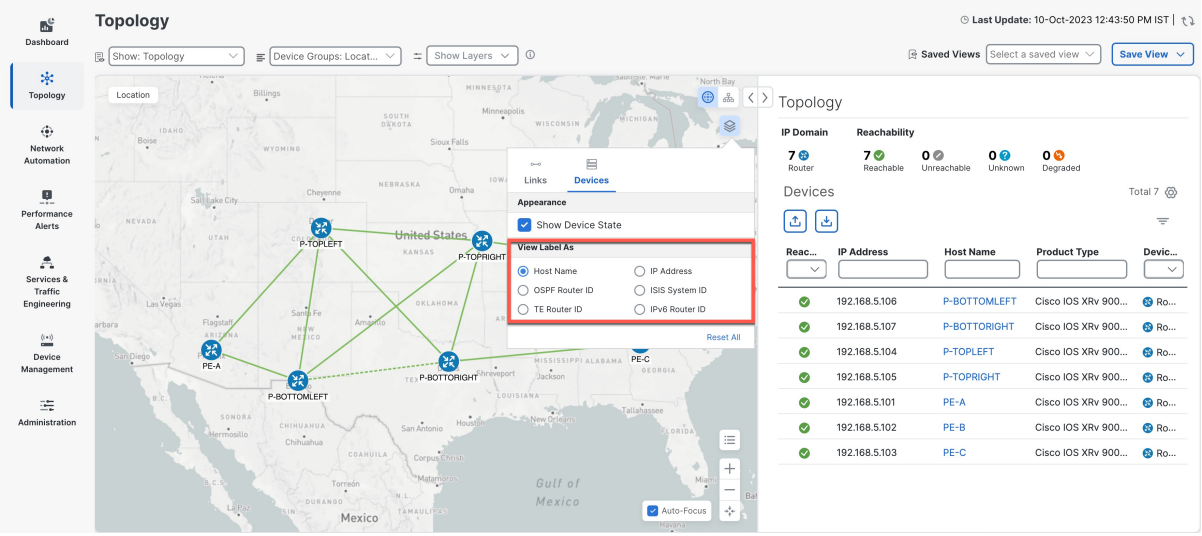
You can customize how you want to identify the devices on your Network Topology. You can use different label types to identify the devices, such as IP Address, OSPF Router ID, or the default option of device host name.

Step 1 From the main menu click **Topology**.

Step 2 Click on the topology map to open the **Display Preference** dialog box.

Step 3 Click **Devices** tab and under **View Label As** select the desired option from the list of labels. You can select only one label for your devices.

Figure 89: Define the Device Label Type



Differentiate Aggregated Links from Single Links

An aggregated link is a type of link that combines multiple physical links or multiple protocols, such as IPv4 and IPv6, into one logical link. This allows for better bandwidth utilization and redundancy. On the topology map, an aggregated link is shown as a dashed line, while a single link is shown as a solid line. This helps to simplify the network topology and show the logical connections between devices.

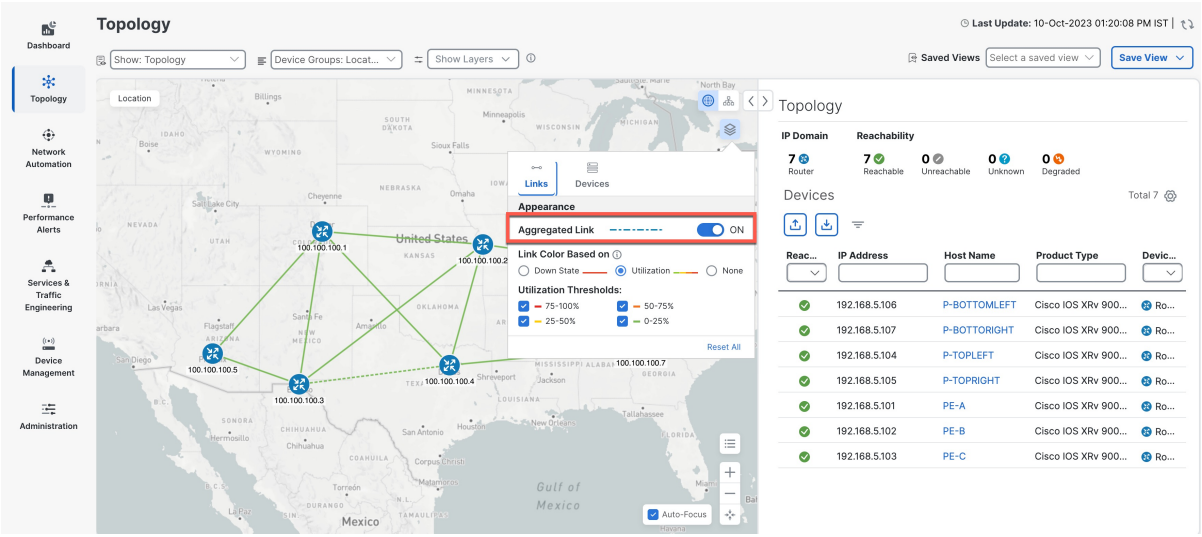
Note Although aggregated, dual stack links show as one single line

Step 1 From the main menu click **Topology**.

Step 2 Click on the topology map to open the **Display Preference** dialog box.

Step 3 Click **Links** tab, toggle to enable the **Aggregated Link** option.

Figure 90: Aggregated Link



Differentiate all Down Links

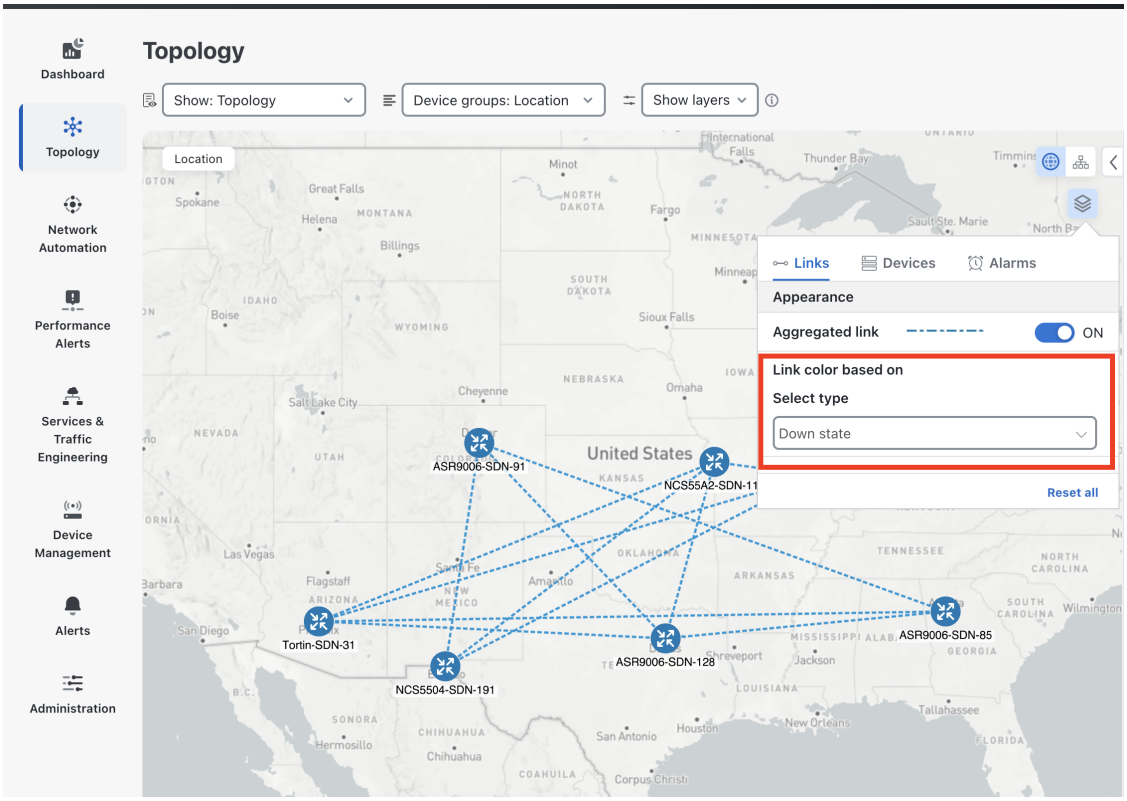
To make it easier to identify the links that are not working, you can set your display preferences to view only links that are down.

Step 1 From the main menu click **Topology**.

Step 2 Click on the topology map to open the **Display Preference** dialog box.

Step 3 Click the **Links** tab and under **Link color based on** select the **Down state** option. All the links that are down will appear in red.

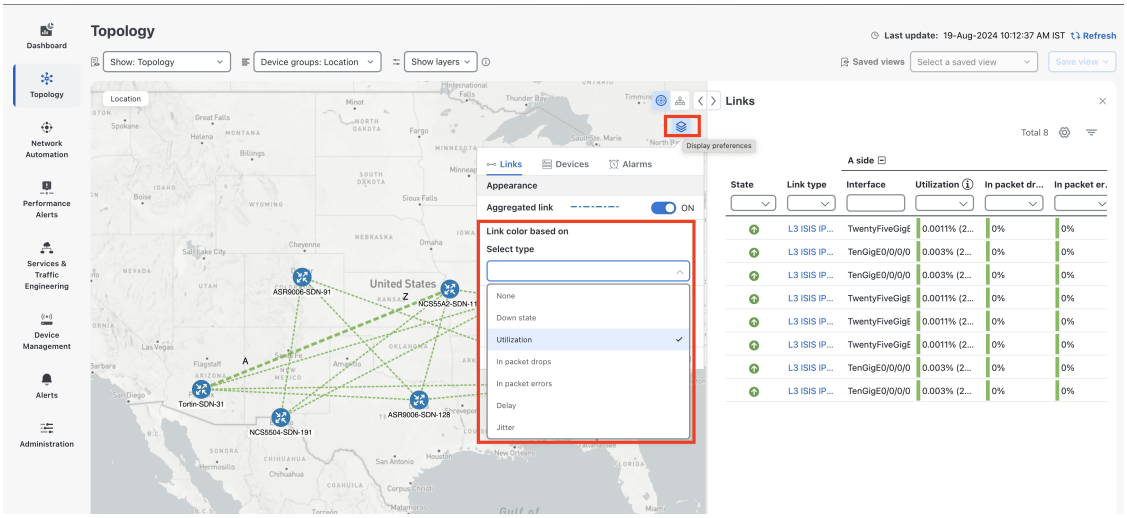
Figure 91: Link color based on Down state



Show Link Health by Color

Link health can be visualized and monitored in the logical and geographical maps. You can assign link colors based on metrics like delay, jitter, packet errors and packet drops.

Note Delay and jitter metrics are available only when Segment Routing Performance Monitoring (SR-PM) is enabled. This requires installing Service Health, which 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 7.0 Service Health Monitoring guide.



The color thresholds can be customized by administrators. Up to three thresholds can be defined for each metric.

To set color thresholds for a metric:

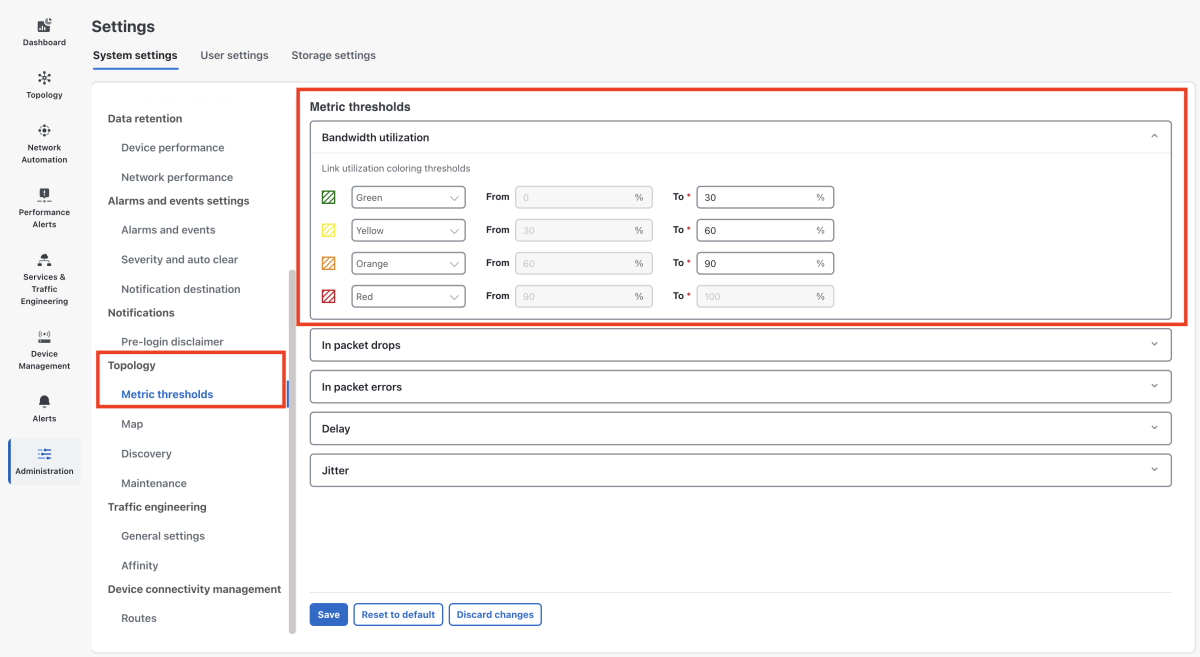
Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings**.

Step 2 Under **Topology**, click the **Metric Thresholds** option.

Step 3 For a metric, define the criteria for coloring the links. Each row defines a color and the percentage range that the color will represent.

- You can enter values in the **To** fields only. Each row begins automatically from the end of the previous row's range.
- The thresholds must be sequential, meaning that each row's range must follow on from the previous row's range. For example, for bandwidth utilization, if the range in the first row is 0-25%, the second row's range must end with a value greater than 25.
- You cannot use the same color for multiple thresholds. For example, you cannot choose **Green** for both the first and second rows.

Figure 92: Metric thresholds for Bandwidth Utilization



Step 4 Click **Save**.

Troubleshoot your Topology Map

To resolve any problems with your topology map, you need to check the network connectivity and configuration of your devices. Ensure that they are online and have the correct IP addresses, subnet masks, gateways, and DNS settings. You also need to make sure that your topology map matches the actual physical layout of your network. This will help you to optimize the performance and accuracy of your topology map.

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 show no links and devices while the rebuild is in progress. They will reappear when the rebuild is finished.

Before you begin

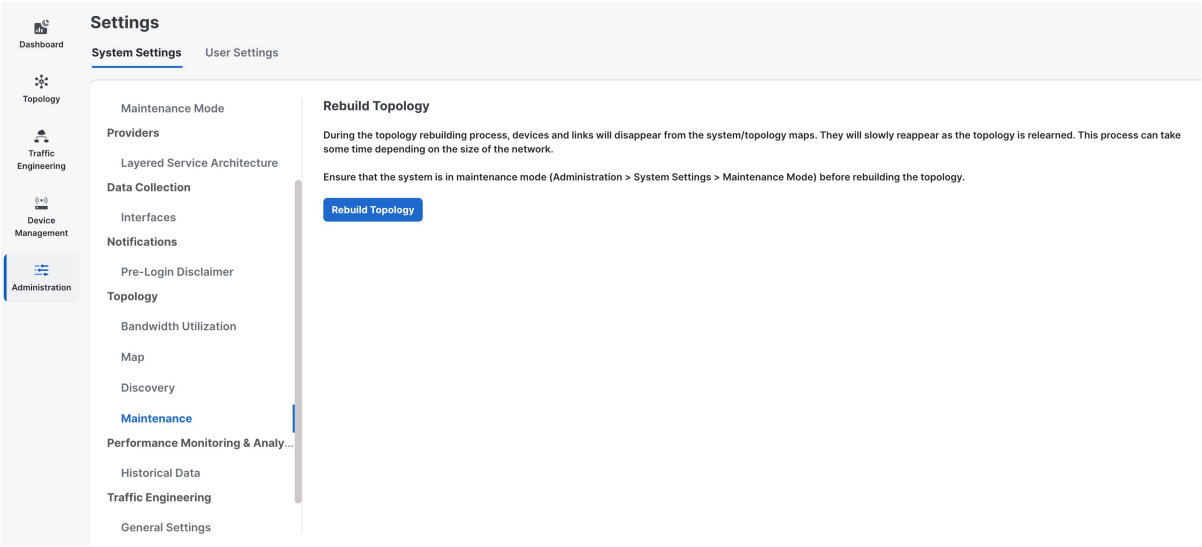
To start the topology rebuild, the system must be in maintenance mode.

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings**.

Step 2 Under **Topology**, click the **Maintenance** option.

Step 3 In the **Rebuild Topology** section, click **Rebuild Topology**.

Figure 93: Rebuild the Topology



Step 4 To confirm your Topology rebuild, in the **Confirm Topology Rebuild** pop-up, click **Rebuild Topology** again.

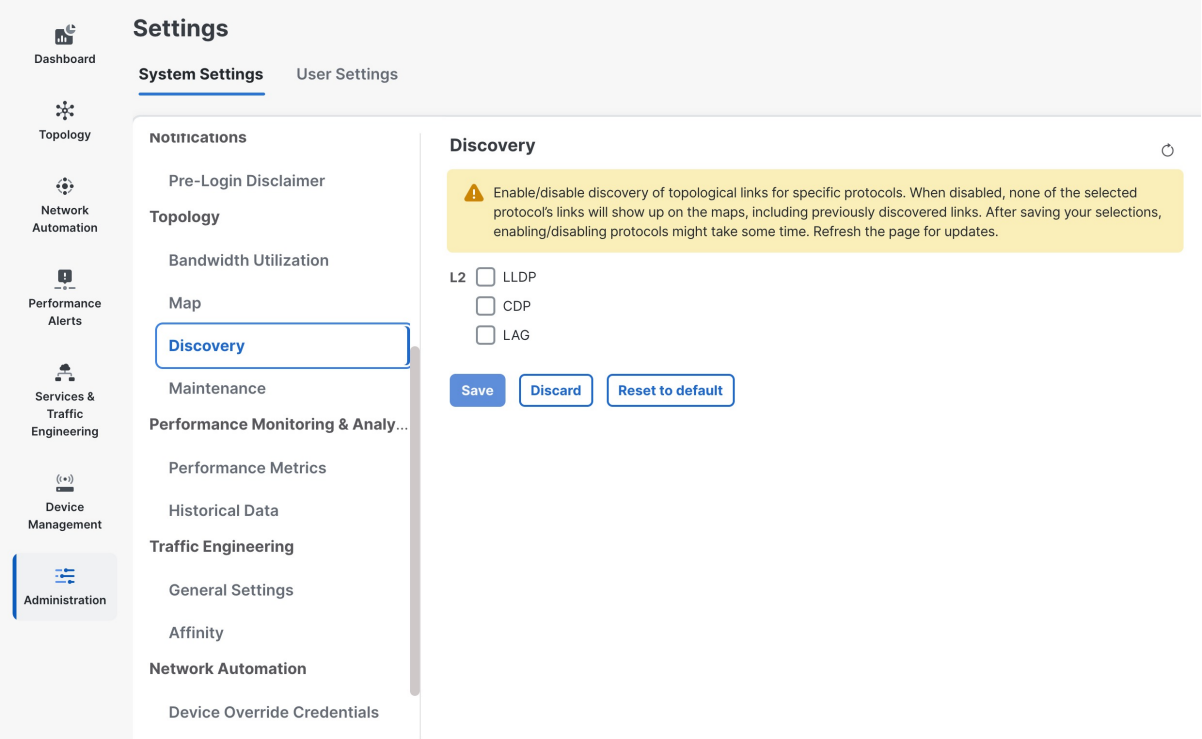
Find Missing L2 Links

If L2 links are missing, it is important to check the protocol settings and ensure that they are enabled. By default, L2 link discovery is not enabled, so you may need to manually enable it in order to discover L2 links. Once the protocol settings are correctly configured, you should be able to discover and view L2 links in your network. For more information refer to Enable or Disable Topology Link Discovery, on page 216.

Step 1 From the main menu, click **Administration** > **Settings** > **System Settings**.

Step 2 Under **Topology**, click the **Discovery** option.

Figure 94: L2 Link Discovery



Step 3 Select the desired option and click **Save**.

Step 4 If the L2 links are not visible, ensure that the following configurations are checked:

a. PCE Configuration

- Configuring the PCE IP Address. Ensure the IP `198.19.1.201` is assigned to one of the loopback interfaces on the device.

```
pce
 address ipv4 198.19.1.201
```

- Configure the API user with the following credentials:

```
api
 user cisco
  password encrypted 121A0C041104
```

- Configure PCE sibling.

  Ensure the sibling PCE is correctly configured and visible.

```
sibling ipv4 11.1.201.202
```

b. Verify the Sibling PCE Connectivity.

Ensure that the sibling PCE is connected

```
RP/0/RP0/CPU0:pce-1#show pce api sibling connection
```

Result:

```
Address:                    11.1.201.202
Connected:                        Yes
```

```
Input buffer size:                  0
Packets in output buffer:           0
```

c. PCC Configuration for PCEP Peering

For the head-end node to become a PCEP peer, the following configurations are necessary:

```
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 Session

Ensure the PCEP session is up and running

- 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
```

Result:

```
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
```

In case the L2 links are still missing, consider rebuilding your topology. Refer to Rebuild the Topology, on page 225

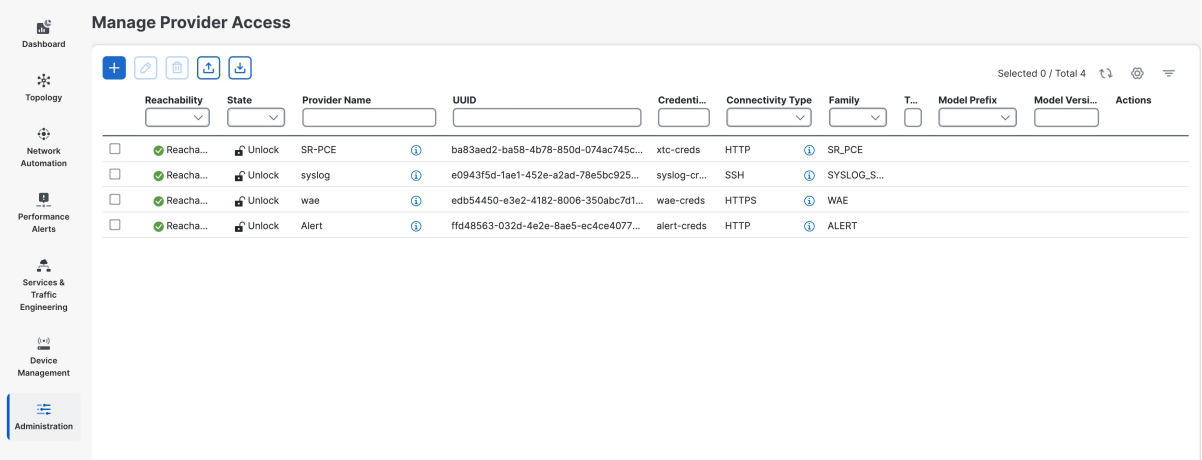
Missing L3 Links

One of the possible reasons for missing L3 links is a device level issue. This means the SR-PCE cannot learn the IGP information for that device. Some of the factors that can cause a device level issue are hardware failure, software bugs, misconfiguration, or interference. To troubleshoot this problem, you should first check the device status and logs for any errors or warnings. Then check the IGP configurations for that device and check if the SR-PCE has that device in its topology.

Step 1 From the main menu, click **Administration** > **Manage Provider Access**.

Step 2 Under **Reachability** column, ensure that the providers are reachable.

Figure 95: Manage Provider Access



Step 3 If the L3 links are not visible, ensure that the following configurations are checked:

- If a link is missing in the topology UI, ensure that the ISIS/OSPF neighbor relationship is up using the below configurations:

  ```
  RP/0/RP0/CPU0:Node-4#show isis neighbors
  ```

  Result:

  ```
  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
  ```

  Result:

  ```
  IS-IS 1 neighbors:
  System Id      Interface        SNPA           State Holdtime Type IETF-NSF
  Node-4         Gi0/0/0/1        *PtoP*         Up    22       L2   Capable
  ```

- Ensure that the link is configured with point-to-point:

  ```
  router isis 1
  interface GigabitEthernet0/0/0/0
    point-to-point
  ```

- Ensure that the link is visible in PCE:

  ```
  show pce ipv4 topology 198.19.1.4
  ```

  Result:

  ```
  Node 30
    Link[2]: local address 10.4.7.4, remote address 10.4.7.7
  ```

In case the L2 links are still missing, consider rebuilding your topology. Refer to Rebuild the Topology, on page 225

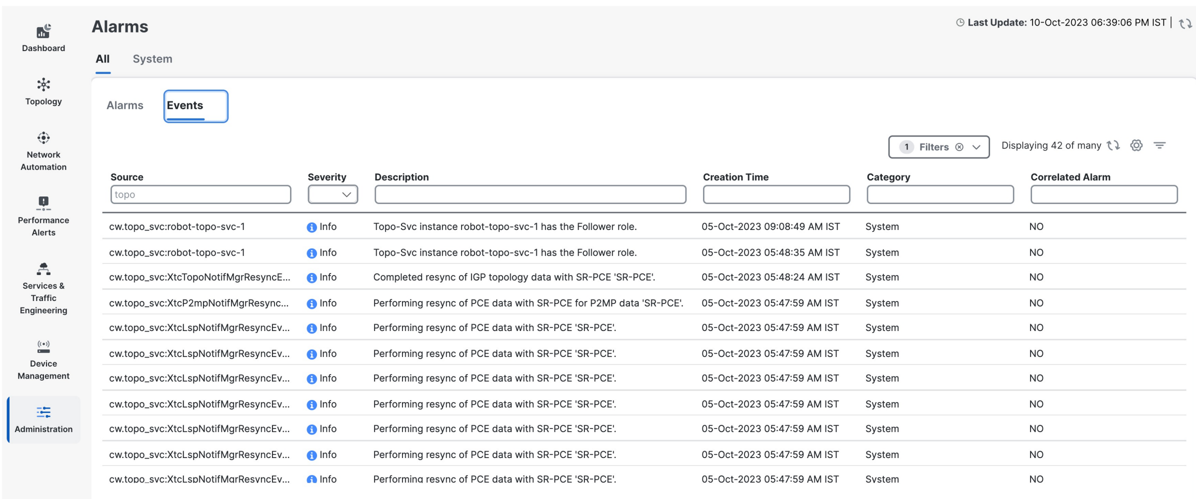
Error Record in Alarm/Events Report of Topology Services

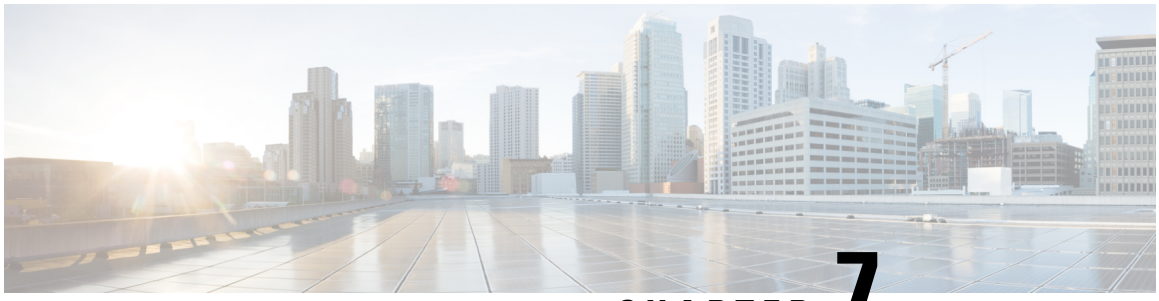
The topology service may encounter errors during its operation, such as missing or incorrect data, communication failures, or configuration issues. These errors are recorded in the alarms/events report, which can help you to diagnose and resolve the problems.

Step 1 From the main menu, click **Administration** > **Alarms**.

Step 2 Enter "topo" in the Source filter. This will display only the alarms and events related to the Topology.

Figure 96: Alarm Events Report of Topology Service





CHAPTER 7

Prepare Infrastructure for Device Management

This section contains the following topics:

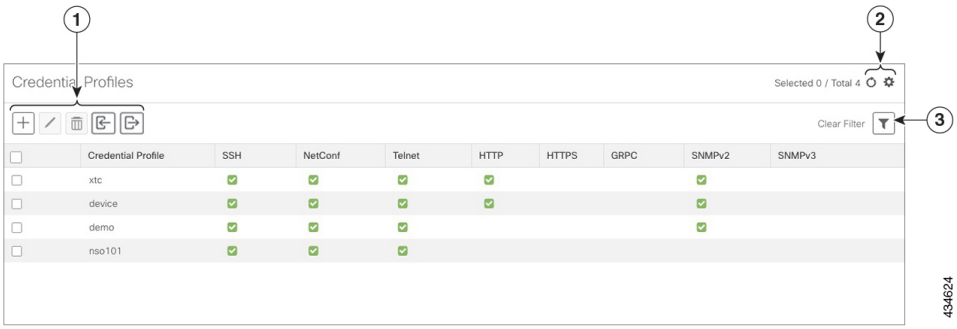
Manage Credential Profiles

Credential profiles are collections of credentials for SNMP, Telnet, SSH, HTTP, and other network protocols. You can have multiple protocols and credentials in a single credential profile.

Using credential profiles lets you automate device configuration changes and monitoring, and communicate with providers. When you add or import devices, or create providers, you specify the credential profile.

From the **Credential Profiles** window, you can create a new credential profile, update the settings configured for an existing profile, or delete a profile. To open this window, choose **Device Management** > **Credential Profiles** from the main menu.

Figure 97: Credentials Profile window



Item	Description
1	Click to add a credential profile. See Create Credential Profiles, on page 232.
	Click to edit the settings for the selected credential profile. See Edit Credential Profiles, on page 236.
	Click to delete the selected credential profile. See Delete Credential Profiles, on page 237.
	Click 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, on page 234.
	Click to export credential profiles to a CSV file. See Export Credential Profiles, on page 237.
2	Click to refresh the **Credential Profiles** window.
	Click to choose the columns to make visible in the **Credential Profiles** window.
3	Click to set filter criteria on one or more columns in the **Credential Profiles** window.
	Click the **Clear Filter** link to clear any filter criteria you may have set.

Create Credential Profiles

Follow the steps below to create a new credential profile. You can then use the profile to apply credentials consistently when you add new devices or providers. You can add as many protocols and corresponding credentials to the profile as you want.

If you have many credential profiles to add, you may find it more efficient to put the information in a CSV file and import the file. See Import Credential Profiles, on page 234.

When creating device credential profiles that contain SNMP credentials, Cisco recommends that the profile contains credentials for the version of SNMP enabled on the device, and that version only. For example: If SNMPv3 is not enabled in the device configuration, do not include SNMPv3 credentials in the device credential profile.

If you plan to use the import and export features and CSV files to create credential profiles in bulk, please note that:

- All the characters in each password or community string entry in every credential profile exported to a CSV file are replaced with asterisks (Export Credential Profiles, on page 237).
- You cannot import credential profiles if the passwords and community strings in the CSV file are blank (see Import Credential Profiles, on page 234).

To maintain network security, Cisco recommends that you use asterisks in place 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 236 to replace the asterisks with actual passwords and community strings.

Step 1 From the main menu, choose **Device Management** > **Credential Profiles**.

Step 2 Click  .

Step 3 In the **Profile Name** field, enter a descriptive profile name. The name can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.

If you will have many credential profiles, make the name as informative as possible because that information will be displayed on the Credential Profiles panel.

Step 4 Select a protocol from the **Connectivity Type** dropdown.

Step 5 Complete the credentials fields described in the following table. The required and optional fields displayed varies with the connectivity type you chose. The values you enter must match the values configured on the device.

Connectivity Type	Fields
SSH	Enter the required **User Name**, **Password**, and **Confirm Password**. The **Enable Password** is optional.
SNMPv2	Enter the required SNMPv2 **Read Community** string. The **Write Community** string is optional.
NETCONF	Enter the required **User Name**, **Password**, and **Confirm Password**.
TELNET **Note** There may be some security limitations when using this protocol.	Enter the required **User Name**, **Password**, and **Confirm Password**. The **Enable Password** is optional.
HTTP	Enter the required **User Name**, **Password**, and **Confirm Password**.
HTTPS	Enter the required **User Name**, **Password**, and **Confirm Password**.
GRPC	Enter the required **User Name**, **Password**, and **Confirm Password**.
gNMI	Enter the required **User Name**, **Password**, and **Confirm Password**.
TL1	Enter the required **User Name**, **Password**, and **Confirm Password**.

Connectivity Type	Fields
SNMPv3	Choose the required **Security Level** and enter the **User Name**. If you chose the NO_AUTH_NO_PRIV **Security Level**, all the fields are optional (except User Name). If you chose the AUTH_NO_PRIV **Security Level**, you must choose an **Auth Type** and enter an **Auth Password**. If you chose the AUTH_PRIV **Security Level**, you must choose an **Auth Type** and **Priv Type**, and enter an **Auth Password** and **Priv Password**. The following SNMPv3 Privacy Types are supported: • CFB_AES_128 • CBC_DES_56 • AES-192 • AES-256 • 3-DES

Step 6 (Optional) Click **+ Add Another** and repeat the previous steps, as needed, for all other protocols and corresponding credentials you want to add to this credential profile.

Step 7 Click **Save**.

Import Credential Profiles

Complete the steps below to create a CSV file that specifies multiple credential profiles and then import it into the Cisco Crosswork application.

Importing credential profiles from a CSV file adds any profiles not already in the database. You cannot import a credential profile that already exists.

If you are re-importing a credential profile CSV file that you previously exported and modified, remember that all the passwords and community strings in the exported credential profile CSV file are replaced with asterisks. You cannot re-import an exported credential profile CSV file with blank passwords. To maintain security, Cisco recommends that you use asterisks in place of real passwords and community strings in the CSV file. After the import, follow the steps in Edit Credential Profiles, on page 236 to replace the asterisks with actual passwords and community strings.

Step 1 From the main menu, choose **Device Management** > **Credential Profiles**.

Step 2 Click  to open the dialog box.

Step 3 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 disk.

b) Open the template using your preferred tool. Begin adding rows to the file, one row for each credential profile.

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;NETCONF;TELNET** in the **Connectivity Type** field and you enter **UserTom;UserDick;UserHarry;** in the **User Name** field, the order of entry determines the mapping between the two fields:

- SSH: UserTom
- NETCONF: UserDick
- TELNET: UserHarry

Also note:

- Be sure to enter SNMP community string information exactly as currently entered on your devices.
- Password and community string information associated with a user ID are stored in plain text in the CSV file you prepare. Be aware of the security implications of this, and apply appropriate safeguards.

Field	Entries	Required or Optional
Credential Profile	The name of the credential profile. For example: .	Required
Connectivity Type	Valid values are: **SSH**, **SNMPv2**, **NETCONF**, **TELNET**, **HTTP**, **HTTPS**, **GRPC** or **SNMPv3**	
User Name	For example:	Required if **Connectivity Type** is **SSH**, **NETCONF**, **TELNET**, **HTTP**, **HTTPS**, **SNMPv3** or **GRPC.**
Password	The password for the preceding **User Name**.	Required if **Connectivity Type** is **SSH**, **NETCONF**, **TELNET**, **HTTP**, **HTTPS** or **GRPC**
Enable Password	Use an Enable password. Valid values are: **ENABLE**, **DISABLE**	
Enable Password Value	Specify the Enable password to use.	
SNMPV2 Read Community	For example: **readprivate**	Required if **Connectivity Type** is **SNMPv2**
SNMPV2 Write Community	For example: **writeprivate**	
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**
SNMPV3 Auth Type	Valid values are **HMAC_MD5** or **HMAC_SHA**	Required if **Connectivity Type** is **SNMPv3** and **SnmpV3 Security Level** is **AuthNoPriv** or **AuthPriv**

Field	Entries	Required or Optional
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	The following 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**

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.

c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

Step 5 With the CSV file selected, click **Import**.

The credential profiles you imported should now be displayed in the **Credential Profiles** window.

Edit Credential Profiles

A credential profile can be shared by multiple devices, even hundreds of devices in a large network. Complete the following procedure to edit credential profile settings.

Before editing any credential profile, it is always good practice to export a CSV backup of the profiles you want to change (see Export Credential Profiles, on page 237).

Step 1 From the main menu, choose **Device Management** > **Credentials**.

Step 2 From the left-hand side of the **Credential Profiles** window, select the profile you want to update, and click  .
The **Edit Profile** window of the selected credential is displayed.

Step 3 Make the necessary changes and then click **Save**.

Export Credential Profiles

Exporting credential profiles stores all the profiles you selected in a CSV file. This is a quick way to make backup copies of your credential profiles. You can also edit the CSV file as needed, and re-import it to add new or modify credential profile data.

The exported credential profiles CSV file does not contain real passwords or community strings. All the characters in the passwords and community strings entries in the credential profiles are replaced with asterisks in the exported CSV file. If you plan on modifying your exported CSV file and then re-importing it, Cisco recommends that you use asterisks in place of real passwords and community strings. After the import, follow the steps in Edit Credential Profiles, on page 236 to replace the asterisks with actual passwords and community strings.

Step 1 From the main menu, choose **Device Management** > **Credential Profiles**.

Step 2 (Optional) In the **Credential Profiles** window, filter the credential profile list as needed.

Step 3 Check the check boxes for the profiles you want to export. Check the check box at the top of the column to select all the profiles for export.

Step 4 Click  . Depending on your browser, you will be prompted to select a path and file name to use when saving the CSV file, or to open it immediately

Delete Credential Profiles

Follow the steps below to delete a credential profile.

Note You cannot delete a credential profile that is associated with one or more devices or providers.

Step 1 Export a backup CSV file containing the credential profile you plan to delete (see Export Credential Profiles, on page 237).

Step 2 Check whether any devices or providers are using the credential profile you plan to delete. You can do this by filtering on the **Credential Profile** column, which is available on both the **Devices** window (choose **Device Management** > **Credential Profiles**) and the Providers window (choose **Administration** > **Manage Provider Access**).

Step 3 Reassign the devices or providers to a different credential profile (for help with this task, see Change the Credential Profile for Multiple Devices, on page 238 and Edit Providers, on page 267).

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 Devices

If you want to change the credential profile for a large number of network devices, you may find it more efficient to make the change by editing a devices CSV file. The basic method is:

1. Export a CSV file containing the devices whose credential profiles you want to change (see Export Device Information to a CSV File, on page 287).
2. Edit the CSV file, changing the credential profile for each device (this credential profile must already exist). Save the edited file.

You will need to make sure that the credential profile to which you are changing already exists. If you have not yet created that credential profile, the CSV import will fail. The credential profile you associate with these devices must also have the authorization credentials for every protocol that was configured for these devices during onboarding. If any credential for a specific protocol configured on the devices is missing from or incorrect in the credential profile, then the CSV import will succeed, but reachability checks will fail for these devices.

Step 1 From the main menu, choose **Device Management** > **Devices**.

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**.

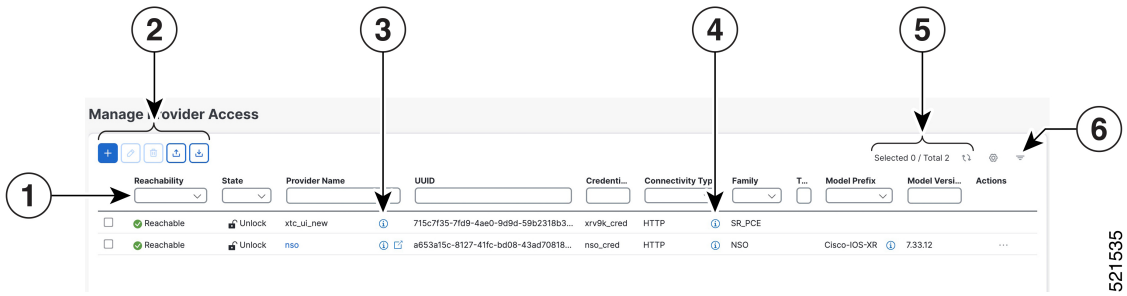
Manage Providers

Cisco Crosswork applications communicate with external providers. Cisco Crosswork stores the provider connectivity details and makes that information available to applications. For more information, see Before You Begin, on page 1.

From the **Providers** window, you can add a new provider, update the settings configured for an existing provider, and delete a particular provider. To open this window, choose **Administration** > **Manage Provider Access**.

Note Wait until the application responds between performing a succession of updates. For example, wait for some time between adding, deleting, or reading providers. Topology services may not receive these changes if you perform these actions too quickly. However, if you find that topology is out of sync, restart the topology service.

Figure 98: Providers Window



Item	Description
1	The icon shown next to the provider in this column indicates the provider's **Reachability**.
2	Click to add a provider. See About Adding Providers, on page 241.
	Click to edit the settings for the selected provider. See Edit Providers, on page 267.
	Click to delete the selected provider. See Delete Providers, on page 268.
	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 Providers, on page 265.
	Click to export a provider to a CSV file. See Export Providers, on page 268.
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 the columns to make visible in the Providers window (see).

Item	Description
6	Click to set filter criteria on one or more columns in the **Providers** window.
	Click the **Clear Filter** link to clear any filter criteria you may have set.

About Provider Families

Cisco Crosswork 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.

The currently supported provider families are shown in the following table.

Table 18: Supported Provider Families

Provider Family	Description
NSO	Instances of Cisco Network Services Orchestrator (Cisco NSO), used to configure network devices. See Add Cisco NSO Providers, on page 244.
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 Cisco SR-PCE Providers, on page 249.
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 261 .
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 262.
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 263
Proxy	Instances of proxy providers. See Add Proxy Providers, on page 264

Provider Dependency

This section explains the provider configurations required for each Cisco Crosswork component.

Table 19: Provider Dependency matrix

Cisco Crosswork 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
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.

About Adding Providers

Cisco Crosswork depends on a variety of providers to perform various functions. For example, Cisco Network Services Orchestrator provides segment routing policies and device information. Features that depend on new providers may be added in the future, and you may need to communicate with more than one instance of a single provider. To access each provider's services, the provider must be added to the Cisco Crosswork application's system configuration.

There are two ways to add providers:

1. **Adding providers via the UI**: This method is explained in Add Providers Through the UI, on page 242. Although this method is the most time-consuming, it is more often used because most deployments will not need a lot of provider instances.
2. **Importing providers from a providers CSV file**: This method is explained in Import Providers, on page 265. Importing a CSV file is useful when you have a lot of provider instances to add or update at one time.

Note that both methods require that you:

- Create a corresponding credential profile, beforehand, so that the Cisco Crosswork applications can access the provider. For help, see Create Credential Profiles, on page 232.
- Know the protocol, IP address, port number, and other information needed to connect with the provider.
- Know any special properties the provider may require during the session startup.

Add Providers Through the UI

Use this procedure to add a new external provider. You can then map the provider to devices.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click  .

Step 3 Enter values for the provider as listed in the following table.

Step 4 When you have complete entries in all of the required fields, click **Save** to add the new provider.

Step 5 (Optional) Repeat to add more providers.

Table 20: Add Provider Fields (*=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 a maximum of 128 alphanumeric characters, plus 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. Choices are: **`NSO`**, **`WAE`**, **`SR-PCE`**, **`ALERT`** and **`SYSLOG_STORAGE`**.
Connection Type(s)	
*** Protocol**	Select the principal protocol that the Cisco Crosswork application will use to connect to the provider. Options include: **`HTTP`**, **`HTTPS`**, **`SSH`**, **`SNMP`**, **`NETCONF`**, **`TELNET`**, and more. 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 as many sets of connectivity details as you want, including multiple sets for the same protocol.

Field	Description
*** Server Details**	Select and provide one of the 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	Enter the amount of time (in seconds) to wait before the connection times out. The default is 30 seconds.
Model Prefix Info	
*** Model**	Required only 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 control how the Cisco Crosswork application interacts with the provider. Not all providers need them, and the number and type of properties vary with the provider family. These properties are documented in topics about adding specific providers elsewhere in this Guide. Please note, however, that the Cisco Crosswork application does not validate provider properties. Make sure the properties you enter are 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.

Field	Description
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.

Add Cisco NSO Providers

This topic explains the steps to add a Cisco NSO provider through the Crosswork UI.

The Cisco Network Services Orchestrator (Cisco NSO) provider functions as the provider for Cisco Crosswork to configure the devices according to their expected functions, including optionally configuring MDT sensor paths for data collection. Cisco NSO provides the important functions of device management, configuration and maintenance services.

Cisco Crosswork also supports Cisco NSO Layered Service Architecture (LSA) deployment. The LSA deployment is constructed from multiple NSO providers, that function as the customer-facing service (CFS) NSO containing all the services, and the resource-facing service (RFS), which contains the devices. Crosswork automatically identifies the NSO provider as CFS or RFS. Only one CFS is allowed. On the **Manager Provider Access** page, the **Type** column identifies the NSO provider as CFS.

Note

- The Cisco NSO sample function packs are provided as a starting point for VPN service provisioning functionality in Cisco Crosswork Network Controller. While the samples can be used “as is” in some limited network configurations, they are intended to demonstrate the extensible design of Cisco Crosswork Network Controller. Answers to common questions can be found on Cisco Devnet and Cisco Customer Experience representatives can provide answers to general questions about the samples. Support for customization of the samples for your specific use cases can be arranged through your Cisco account team. See View Installed NSO Function Packs, on page 248 to monitor the state of the installed NSO function packs.
- The NSO Function Pack deployment via Crosswork UI is supported for NSO system installation and as a root user.

Attention

Crosswork does not scan NSO continuously for NSO device status changes. New device addition to NSO is discovered by Crosswork only when there is an explicit action from Crosswork towards NSO.

To onboard newly added devices from NSO to Crosswork:

- 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 to rescan NSO.

Note that you can import several providers at the same time by preparing a CSV file with the details of all the providers and importing it into Crosswork (see Import Providers, on page 265).

Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider (see Create Credential Profiles, on page 232).
- Know the name you want to assign to the Cisco NSO provider.
- Know the Cisco NSO NED device models and driver versions used in your topology. You can find the Cisco NSO version using the `version` command.
- Know the Cisco NSO server IP address or FQDN (Domain name and host name). When NSO is configured with HA, the IP address would be management VIP address.
- Confirm Cisco NSO device configurations. For more information, see Sample Configuration for Cisco NSO Devices, on page 281.
- The NSO cross launch feature is not available for user roles with read-only permissions.

For NSO LSA deployment:

- If you plan to add a NSO LSA provider, you must first enable LSA settings. See Enable Layered Service Architecture (LSA), on page 247 for details.
- If you forgot to enable the LSA setting or misconfigures the provider property values, please perform the recovery steps mentioned in NSO LSA Setup Recovery, on page 248.
- The RFS node IP addresses used on the CFS must match with the IP addresses on the Crosswork UI. A mismatch will generate the error "*LSA cluster is missing RFS providers*".
- In case of the CFS node, only the **`forward`** property key is used.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click  .

Step 3 Enter the following values for the Cisco NSO provider fields:

a) Required fields:

- **Provider Name**: Enter a name for the provider.
- **Credential Profile**: Select the previously created Cisco NSO credential profile.
- **Family**: Select **`NSO`**.
- **Protocol**: Select **`HTTPS`** and/or **`SSH`**. For more information, see Provider Dependency, on page 240.

  Note To use the **Backup NSO** option during backup, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail.

- **Server Details**: Enter either the IP address (IPv4 or IPv6) or FQDN (Domain name and Host name) of the server.
- **Port**: 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.
- **Model**: Select the model (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.

Note If you set the **Site location** parameter in NSO, you can determine if geo-fencing is violated during testing when Crosswork and the active NSO are not in the same site location. Crosswork will also raise and clear alarms if a geo-fence violation is detected.

Important When you modify or update the NSO provider IP address or FQDN, you need to detach devices from corresponding virtual data gateway, and reattach them. If you fail to do this, the provider changes will not be reflected in MDT collection jobs.

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the Cisco NSO server. The default is 30 seconds.

c) **Provider Properties**: Enter one of the following key/value pairs in the first set of fields:

Property Key	Value
`forward`	**`true`** This property is necessary when using the Cisco Crosswork Network Controller solution to allow provisioning operations within the UI and to enable the northbound interface to NSO via the Crosswork API gateway. **Note** The default value of **`forward`** is "false". If this is not changed, the devices added to Crosswork will not be added to NSO. This setting is used in conjuction with the **Edit Policy** option (see Edit NSO provider policy, on page 249).
`nso_crosslaunch_url` **Note** This property is used only for NSO standalone provider.	Enter the URL for cross-launching NSO in the format: **`https://<NSO IP address/FQDN>: port number`** To enable cross-launch of the NSO application from the Crosswork UI. 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 This property is used only for NSO LSA provider.
	Enter the RFS ID in the format: **`/rfc-x`**, where **`x`** refers to the number of the RFS node.
	`Example (for RFS node 1):`
	`input_url_prefix: /rfc-1`

Step 4 When you have completed entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

What to do next

(Optional) The site name can be configured for NSO from the NCS backend, and it will be displayed as a read-only value on the NSO provider in the Crosswork UI.

To configure the NSO site name:

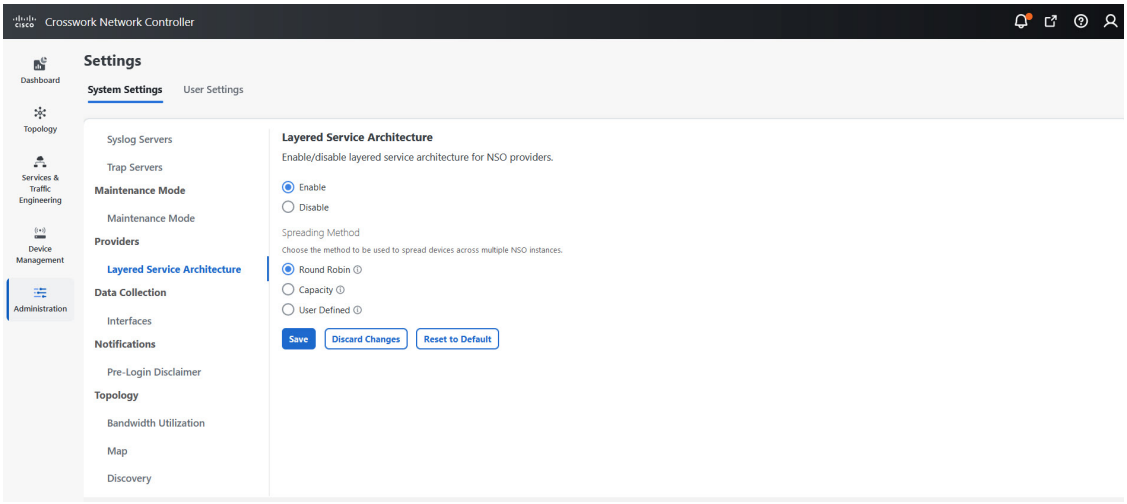
1. Login into ncs_cli in config mode.
2. Set `hcc dns member master ip-address nso1-mgmt-IP location site1-location`
3. Set `hcc dns member standby ip-address nso2-mgmt-IP location site2-location`
4. Commit

Enable Layered Service Architecture (LSA)

This procedure is applicable only when you have opted for Cisco NSO LSA deployment to add arbitrarily many device nodes for improved memory and provisioning throughput.

Step 1 From the main menu, select **Administration** > **Settings** > **System Settings** > **Layered Service Architecture**.

Figure 99: Enabling Layered Service Architecture Window



Step 2 Select **Enable**.

Step 3 Select the method to spread the devices across multiple NSO instances:

- **Round Robin** - Even distribution of devices to RFS nodes in a cyclical manner (for example, Device 1 to RFS1, Device 2 to RFS2, and so on).
- **Capacity** - The number of devices are assigned to each RFS instance based on its total capacity.
- **User Defined** - Devices are assigned to the NSO providers specified for the device in the device settings. For more information, see Add Devices Through the User Interface, on page 282.

Step 4 Click **Save**.

Note Once you have saved the settings, you cannot disable it without removing all the NSO providers.

NSO LSA Setup Recovery

This topic explains the steps for NSO LSA setup recovery in case of any misconfigurations.

Step 1 Remove the NSO providers and associated devices on Device Management window.

Step 2 Clean up the associated services on the Cisco NSO application.

Step 3 Enable the LSA settings and add the NSO LSA provider with correct property values.

Step 4 Add the NSO providers and devices again to Crosswork, and map them to the Crosswork Data Gateway.

Step 5 Perform the sync operation on the NSO nodes (RFS and CFS) again to sync the devices correctly.

This will recover the functionality as expected.

View Installed NSO Function Packs

Cisco Crosswork allows you to monitor the status of the installed NSO Function Packs.

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

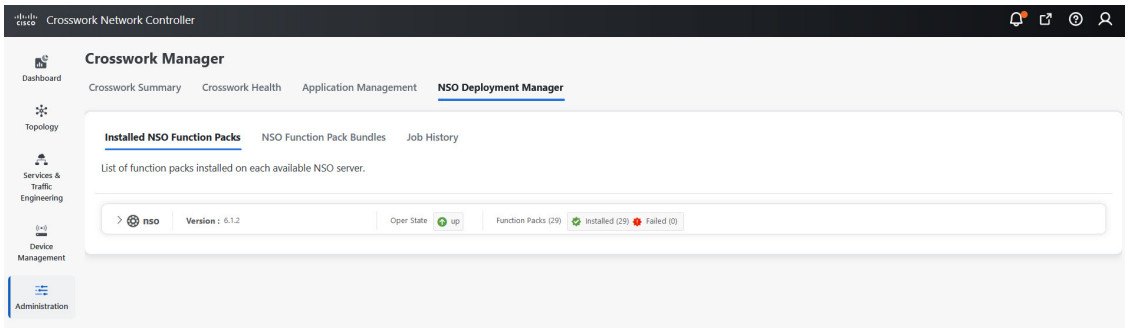
Step 2 On the **Crosswork Manager** window, select the **NSO Deployment Manager** tab.

The **Installed NSO Function Packs**, **NSO Function Pack Bundles**, and **Job History** tabs are displayed.

Note You can also navigate here from the NSO provider entries in the **Providers** window (click **Actions** > **View Function Packs**).

The **Installed NSO Function Packs** tab displays a list of NSO function pack bundles deployed on the configured NSO server.

Figure 100: 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 as **Up** or **Down**, description, and version.

Edit NSO provider policy

To edit an NSO provider policy, perform the following:

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 On an NSO provider, click **Actions** > **Edit policy details**.

The **Edit policy details** window for the selected NSO provider is displayed.

Step 3 Edit the configuration fields to match the requirements of your environment.

Note Set **Onboard from** to **TRUE**) to trigger Crosswork to rescan NSO.

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

Add 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 the Cisco Crosswork applications. At least one SR-PCE provider is required in order to learn and discover SR policies, Layer 3 links, and devices. You have the option to configure a second SR-PCE as a backup. Both SR-PCE devices must be connected to the same network as Crosswork Network Controller and does not support managing more than one domain.

Note To enable Cisco Crosswork application access to an SR-PCE as an SDN controller on the management domain, SR-PCE needs to be added as a provider.

Follow the steps below to add (through the UI) one or more instances of Cisco SR-PCE as providers.

Before you begin

You will need to:

- Configure a device to act as the SR-PCE. See SR configuration documentation for your specific device platform to enable SR (for IS-IS or OSPF protocols) and configure an SR-PCE (for example: *Segment Routing Configuration Guide for Cisco NCS 540 Series Routers*).
- Create a credential profile for the Cisco SR-PCE provider (see Create Credential Profiles, on page 232). This should be a basic HTTP text-authentication credential (currently, MD5 authentication is not supported). If the Cisco SR-PCE server you are adding does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP protocol.
- Know the name you want to assign to the Cisco SR-PCE provider. This is usually the DNS hostname of the Cisco SR-PCE server.
- Know the Cisco SR-PCE server IP address.
- Know the interface you want to use to communicate between Cisco SR-PCE and the Cisco Crosswork application server.

- Determine whether you want to auto-onboard the devices that Cisco SR-PCE discovers and, if so, whether you want the new devices to have their management status set to **`off`**, **`managed`** or **`unmanaged`** when added.
- If you plan to auto-onboard devices that the Cisco SR-PCE provider discovers, and set them to a managed state when they are added to the database:
  - Assign an existing credential profile for communication with the new managed devices.
  - The credential profile must be configured with an SNMP protocol.
- For high availability, ensure that you set up two separate Cisco SR-PCE providers with unique names and IP addresses, but with matching configurations .

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click  .

Step 3 Enter the following values for the SR-PCE provider fields:

a) Required fields:

- **Provider Name**: Name of the SR-PCE provider.
- **Credential Profile**: Select the previously created Cisco SR-PCE credential profile.
- **Family**: Select **`SR_PCE`**. All other options should be ignored.
- **Protocol**: Select **`HTTP`**.
- **Server Details**: Enter either the IP address (IPv4 or IPv6) or FQDN (Domain name and Host name) and subnet mask of the server.
- **Port**: Enter **`8080`** for the port number.
- **Provider Properties**: Enter one of the following key/value pairs in the first set of fields:

Property Key	Value
auto-onboard	**off** **Note** Use this option if you plan to manually (via UI or CSV import) enter all of your network devices. When devices are discovered, the device data is recorded in the Cisco SR-PCE database, but is not registered in Crosswork Network Controller Inventory Management database.
	unmanaged If this option is enabled, 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 If this option is enabled, 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**. 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.
device-profile	The name of a credential profile that contains SNMP credentials for all the new devices. **Note** This field is necessary only if **auto-onboard** is set to **managed**. If the **auto-onboard** is set to **managed** and there is no valid **device-profile** set, the device will be onboarded as **unmanaged** instead.
outgoing-internal	**eth1** **Note** You have to set this only if you want to enable Cisco Crosswork application access to SR-PCE via the data network interface when using the two NIC configuration.
preferred-stack	**ipv4** or **ipv6** or **NOT SET**. This property is applicable only for dual stack deployments.

Property Key	Value
`topology`	**`off`** or **`on`**. This is an optional property. If not specified, the default value is **`on`**. If value is specified as **`off`**, it means that L3 topology is not accessible for the SR-PCE provider.
`pce`	**`off`** or **`on`**. This is an optional property. If not specified, the default value is **`on`**. If value is specified as **`off`**, it means that LSPs and policies are not accessible for the SR-PCE provider.

Note Topology can be visualized even with **`auto-onboard`** as **`off`** and no **`device-profile`**.

Note If **managed** or **unmanaged** options are set and you want to delete a device later, you must do one of the following:.

- 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.

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the SR-PCE server. The default is 30 seconds.

Step 4 When you have completed entries in all of the required fields, click **Save** to add the SR-PCE provider.

Step 5 Confirm that the SR-PCE provider shows a green Reachability status without any errors. You can also view the Events window (**Administration** > **Events**) to see if the provider has been configured correctly.

Step 6 Repeat this process for each SR-PCE provider.

Note It is not recommended to modify auto-onboard options once set. If you need to modify them, do the following:

1. Delete the provider and wait until deletion confirmation is displayed in the Events window.
2. Re-add the provider with the updated auto-onboard option.
3. Confirm the provider has been added with the correct auto-onboard option in the Events window.

What to do next

- If you entered the **auto-onboard/off** pair, navigate to **Device Management** > **Network Devices** to add a devices.
- If you opted to automatically onboard devices, navigate to **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

You can find reachability issues raised in the Events table and reachability status in the **Providers** window (see Get Provider Details, on page 266). If the SR-PCE goes down, all links in the topology will display with the last known state since the SR-PCE cannot send any notification updates. When the SR-PCE becomes reachable again, a message will show in the **Events** table ( ) that SR-PCE is reconnected and the topology will be updated accordingly. If you find that the SR-PCE goes down for an extended amount of time, it is not syncing, updates are not happening, then delete the SR-PCE and add it back (when connectivity returns) using the UI:

1. Execute the following command:

   ```
   # process restart pce_server
   ```

2. From the UI, navigate to **Administration** > **Manage Provider Access** and delete the SR-PCE provider and then add it back again.

You can also troubleshoot reachability as follows:

Step 1 Check device credentials.

Step 2 Ping the provider host.

Step 3 Attempt a connection using the protocols specified in the connectivity settings for the provider. For an SR-PCE provider, it is typically HTTP and port 8080.

Step 4 Check your firewall setting and network configuration.

Step 5 Check the Cisco SR-PCE host or intervening devices for Access Control List settings that might limit who can connect.

Multiple Cisco SR-PCE HA Pairs

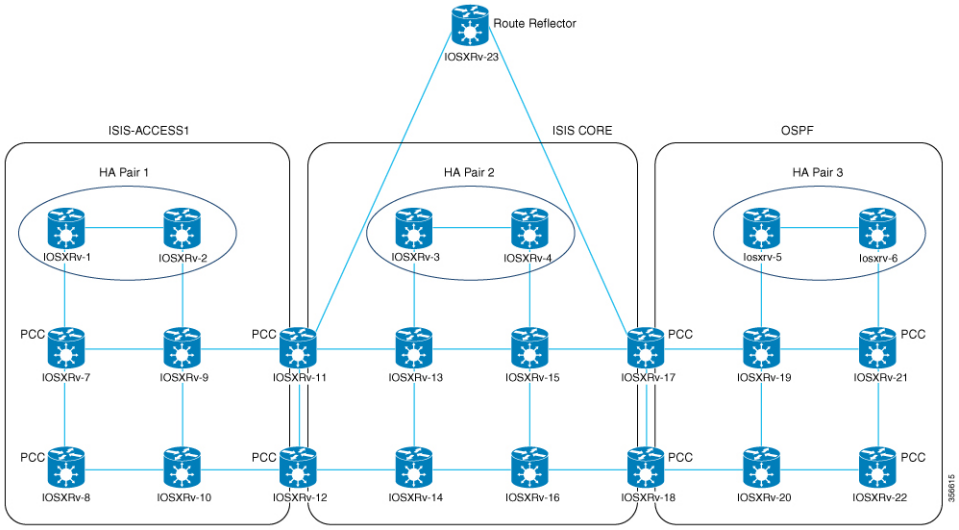
You can set up to eight Cisco SR-PCE HA pairs (total of 16 SR-PCEs) to ensure high availability (HA). Each HA pair of Cisco SR-PCE providers must have matching configurations, supporting the same network topology. In HA, if the primary SR-PCE becomes unreachable, Cisco Crosswork Optimization Engine uses the secondary SR-PCE to discover the network topology. If this pair fails, then 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 Pairs

In the case of multiple SR-PCE HA pairs, each SR-PCE pair sees the same topology but manages and only knows about tunnels created from its Path Computation Clients (PCCs). The following figure is a sample of a three SR-PCE HA pair topology. Note the following:

- HA Pair 1—PCE iosxrv-1 and iosxrv-2 provisions and discovers *only* 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 provisions and discovers *only* 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 provisions and discovers *only* about tunnels whose headends are iosxrv-21, and iosxrv-22. Note that iosxrv-19, and iosxrv-20 are not PCC routers.

Figure 101: Sample 3 HA Pair Topology



Note If any of the SR-PCEs are included in a *subset* of the main network topology, then that SR-PCE provider must be added with the Property Key as **topology** and the Property Value as **off**. When this value is set, then this SR-PCE will not be used to learn the topology.

Configure HA

The following configurations must be done to enable each pair of HA Cisco SR-PCE providers to be added in Cisco Crosswork Optimization Engine.

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 the following commands on *each* of the Cisco SR-PCE devices:

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.

Issue the following 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 synchronization between SR-PCEs in HA are intact:

```
#show tcp brief | include <remote-SR-PCE-router-id>
```

Confirm that following 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 following 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
```

- Cisco Crosswork SR-PCE initiated—An SR-TE policy that is configured using Cisco Crosswork. SR-PCE delegation is random per policy.

Note Only SR-TE policies or RSVP-TE tunnels created by Cisco Crosswork Optimization Engine can be modified or deleted by Cisco Crosswork Optimization Engine.

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 Cisco Crosswork.
  - 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 Cisco Crosswork Optimization Engine, 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 Cisco Crosswork Optimization Engine, then topology information will not be accurate in Cisco Crosswork Optimization Engine. When this happens, fix the connectivity issue or delete both SR-PCEs from the Provider page and re-add the one that is reachable.

SR-PCE Configuration Examples

The following configurations are *examples* to guide you in a multiple SR-PCE setup for HA. Please modify accordingly.

Sample redundant SR-PCE configuration (on PCE with Cisco IOS-XR 7.x.x)

```
pce
 address ipv4 192.168.0.7
 state-sync ipv4 192.168.0.6
 api
  sibling ipv4 192.168.0.6
```

Sample redundant SR-PCE Configuration (PCC)

```
segment-routing
 traffic-eng
  pcc
   source-address ipv4 192.0.2.1
   pce address ipv4 192.0.2.6
    precedence 200
   !
   pce address ipv4 192.0.2.7
    precedence 100
   !
   report-all
   redundancy pcc-centric
```

Sample 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 209.165.255.1
  peer ipv4 209.165.0.6
   precedence 200
  !
  peer ipv4 209.165.0.7
   precedence 100
  !
  stateful-client
   instantiation
   report
   redundancy pcc-centric
   autoroute-announce
  !
 !
 auto-tunnel pcc
  tunnel-id min 1000 max 1999
 !
!
```

Sample SR-TM Configuation

```
telemetry model-driven
 destination-group crosswork
  address-family ipv4 198.18.1.219 port 9010
   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 and Bandwidth Optimization function packs 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 Cisco Crosswork Optimization Engine **to all the headend routers via NSO**

```
telemetry model-driven
  destination-group CW_43dc8a5ea99529715899b4f5218408a785e40fce
    vrf default
    address-family ipv4 172. 19.68.206 port 31500
      encoding self-describing-gpb
      protocol top
    !
  !
destination-group CW_4b3c69a200668b0a8dc155caff295645c684a8f8
  vrf default
  address-family ipv4 172. 19.68.206 port 31500
    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 (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

PCCs can support delegation and reporting of both RSVP-TE tunnels and SR policies to SR-PCE. In order for both to be supported on the same PCC, two separate PCEP connections must be established with the SR-PCEs. Each PCEP connection must have a distinct source IP address (Loopback) on the PCC.

The following is a Cisco IOS-XR configuration example of PCEP connections for RSVP-TE, where 192.168.0.2 is the PCEP session source IP for RSVP-TE tunnels delegated and reported to SR-PCE. It is a loopback address on the router. Two SR-PCEs are configured for PCEP sessions, where the first will be preferred for delegation of RSVP-TE tunnels due to precedence. Auto-tunnel PCC is configured with a range of tunnel IDs that will be used for assignment to PCE-initiated RSVP-TE tunnels like those created in 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

Cisco WAN Automation Engine (Cisco WAE) providers supply traffic and topology analysis to the Cisco Crosswork applications. 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.

Follow the steps below to use the UI to add one or more instances of Cisco WAE as providers. You can also add providers using CSV files (see Import Providers, on page 265).

Before you begin

You will need to:

- Create a credential profile for the Cisco WAE provider (see Create Credential Profiles, on page 232). This should be a basic HTTP/HTTPS text-authentication credential (currently, MD5 authentication is not supported). If the Cisco WAE server you are adding does not require authentication, you must still supply a credential profile for the provider, 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.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click  .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name**: Name of the Cisco WAE provider.
- **Credential Profile**: Select the previously created credential profile.
- **Family**: Select **`WAE`**.
- **Protocol**: Select **`HTTP`** or **`HTTPS`** respectively as per the credential profile you are using.
- **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the server.
- **Port**: Enter the port number (usually, **`8080`** for HTTP, and **`8843`** for HTTPS).

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

Step 4 When you have completed entries in all of the required fields, click **Save** to add the provider.

Add Syslog Storage Providers

Storage providers supply storage for data collected during Playbook execution.

Follow the steps below to use the UI to add one or more storage providers. You can also add providers using CSV files (see Import Providers, on page 265).

Before you begin

You will need to:

- Create a credential profile for the storage provider (see Create Credential Profiles, on page 232). 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.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click  .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name**: Name of the storage provider.
- **Credential Profile**: Select the previously created storage credential profile.
- **Family**: Select **`SYSLOG_STORAGE`**.
- **Protocol**: Select **`SSH`** to be protocol that Cisco Crosswork application will use to connect to the provider.
- **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the server.
- **Port**: Enter the port number (usually, **`22`** for SSH.
- **Provider Properties**: Enter the following key/value pair in these fields:

Property Key	Property Value
`DestinationDirectory`	The absolute path where the collected data will be stored on the server. For example: **`/root/cw-syslogs`**

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the storage server.

Step 4 When you have completed entries in all of the required fields, click **Save** to add the syslog storage provider.

Add an Alert Provider

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.

Follow the steps below to use the UI to add an alert provider. You can also add the alert provider by importing a CSV file (see Import Providers, on page 265).

Currently, only one alert provider is supported.

Before you begin

You will need to:

- Create a credential profile for the alert provider (see Create Credential Profiles, on page 232). This should be a basic HTTP text-authentication credential (currently, MD5 authentication is not supported). If the provider does not require authentication, you must still supply a credential profile for the provider, but 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 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 **Property Value** field.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click  .

Step 3 Enter the following values for the provider fields:

a) Required fields:

- **Provider Name**: Name of the alert provider.
- **Credential Profile**: Select the previously created alert provider credential profile.
- **Family**: Select **`ALERT`**.
- **Protocol**: **`HTTP`** is pre-selected.
- **IP Address/ Subnet Mask**: Enter the IP Address (IPv4 or IPv6) and subnet mask of the alert server.
- **Port**: Enter the port number (usually, 80 for HTTP).
- **Provider Properties**: The **`alertEndpointUrl`** property key name 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.

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the alert server.

Step 4 When you have completed entries in all of the required fields, click **Save** to add the alert provider.

Add Proxy Providers

This section explains how to add a proxy provider in Crosswork. Crosswork supports the addition of the following proxy providers:

- Cisco NSO
- Cisco Optical Network Controller (ONC) version 1.0

The NSO APIs can be directly accessed if NSO is configured with an externally accessible IP address. However, if NSO is deployed in the same private network as the Crosswork network, then it will be reachable only through the Crosswork interface. Proxy providers enables you to use Crosswork interface to perform service provisioning with NSO.

Before you begin

You will need to:

- Create a credential profile for the Proxy provider (see Create Credential Profiles, on page 232). This should be a basic HTTP or HTTPS text-authentication credential.
- Know the name of the Resource Facing Service (RFS) node 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 that the Cisco NSO providers are added. For more information, see Add Cisco NSO Providers, on page 244.
- In case of NSO proxy provider, please create a credential profile with **HTTP/HTTPS** with **Basic Authentication**.
- In case of ONC 1.0 proxy provider, please create a credential profile with **HTTPS** with **Basic Authentication**.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click  .

Step 3 Enter the following values for the provider fields:

- **Provider Name**: Name of the Proxy provider.
- **Credential Profile**: Select the previously created credential profile.

Note In case of ONC provider, please select the credential profile configured with ONC TAPI APIs. This is not the ONC UI credentials.

- **Family**: Select **PROXY**.
- **Protocol**: Select **HTTP** or **HTTPS**.
- **IP Address/ Subnet Mask**: Enter the IP address (IPv4 or IPv6) and subnet mask of the NSO cluster or the ONC 1.0 cluster VIP.
- **Port**: Enter the port number (usually, **30603** for HTTPS).
- **Timeout**: (Optional) The amount of time (in seconds) to wait before timing out the connection to the server. The default is 30 seconds.

Step 4 Under Provider Properties, enter the following properties:

Table 21: Provider Properties for NSO proxy provider

Property Key	Property Value
`forward`	`true`
`input_url_prefix` **Note** This property is 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 22: Provider Properties for ONC 1.0 proxy provider

Property Key	Property Value
`forward`	`true`
`input_url_prefix`	`/onc-tapi`
`output_url_prefix`	`/crosswork/onc-tapi`

Step 5 When you have completed entries in all of the required fields, click **Save** to add the provider.

Import Providers

Complete the steps below to create a CSV file that specifies providers and then import it into the Cisco Crosswork application.

Importing providers from a CSV file adds any providers not already in the database, and updates any providers with the same name as an imported provider. For this reason, it is a good idea to export a backup copy of all your current providers before an import (see Export Providers, on page 268).

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click  to open the **Import CSV File** dialog box.

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

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.

c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

Step 5 With the CSV file selected, click **Import**.

The provider information you imported should now be displayed in the **Providers** window.

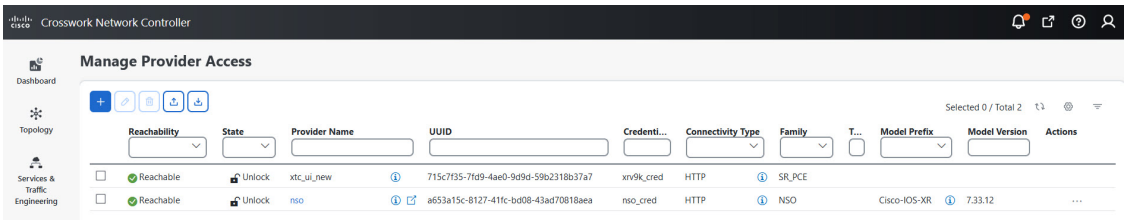
Step 6 Resolve any errors reported during the import and check provider details to confirm connection.

Get Provider Details

Use the **Providers** window to get details about your providers and to check on their reachability.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.
For each provider configured in the Cisco Crosswork application, the **Providers** window lists information such as the provider's name, universally unique identifier (UUID), associated credential profile and more, as shown in the figure below.

Figure 102: Providers Window



Step 2 The icons in the **Reachability** column indicate whether a provider is reachable via the listed connectivity protocols.

Cisco Crosswork application checks provider reachability immediately after a provider is added or modified. Other than these events, Crosswork Change Automation and Health Insights checks reachability every 5 minutes and Crosswork Optimization Engine checks SR-PCE reachability about every 10 seconds.

Step 3 Get additional details for any provider, as follows:

a) In the **Provider Name** column, click the ⓘ to view provider-specific key/value properties.

b) In the **Connectivity Type** column, click the ⓘ to view detailed connectivity information for the provider, such as provider-specific protocol, IP format, IP address, port, and timeout information.

c) In the **Model Prefix** column, click the ⓘ to view the supported NED version(s) for a Cisco Network Services Orchestrator (Cisco NSO) provider's configured NED model prefix(es).

d) When you are finished, click ✕ to close the details window.

If you are running into Cisco SR-PCE reachability problems, see Cisco SR-PCE Reachability Issues, on page 253. Check that HTTP and port 8080 is set.

For general provider reachability problems, you can troubleshoot as follows:

a. Ping the provider host.

b. Attempt a connection using the protocols specified in the connectivity settings for the provider. .

The following CLI command can be used 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. Check the provider host or intervening devices for Access Control List settings that might limit who can connect.

Edit Providers

When editing provider settings, be aware that a provider can be mapped to many devices, even thousands of devices in a large network.

Note

- Before making any changes to a provider configuration you should be certain that you understand the full impact of the change. If you are unsure about the potential risk of making a change, contact Cisco services for guidance.
- See Add Cisco SR-PCE Providers, on page 249 before modifying an SR-PCE provider. There are additional steps that must be done when editing an SR-PCE provider.

.

Before editing any provider, it is always good practice to export a CSV backup of the providers you want to change (see Export Providers, on page 268).

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 In the **Providers** window, choose the provider you want to update and click .

Step 3 Make the necessary changes and then click **Save**.

Step 4 Resolve any errors and confirm provider reachability.

Delete Providers

Follow the steps below to delete a provider.

You are alerted when you try to delete a provider that is associated with one or more devices or credential profiles.

Step 1 Export a backup CSV file containing the provider you plan to delete (see Export Providers, on page 268).

Step 2 (Optional) Check whether any devices are mapped to the provider and change the provider before deletion.

a) From the main menu, 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) Check the check box for 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 Delete the provider as follows:

a) From the main menu, choose **Administration** > **Manage Provider Access**.

b) In the **Providers** window, choose the provider(s) that you want to delete and click .

c) In the confirmation dialog box, click **Delete**.

Export Providers

You can quickly 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.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 (Optional) In the **Providers** window, filter the provider list as needed.

Step 3 Check the check boxes for the providers you want to export. Check the check box at the top of the column to select all the providers for export.

Step 4 Click . Depending on your browser, you will be prompted to select a path and file name to use when saving the CSV file, or to open it immediately.

Manage Tags

Use the **Tag Management** window to manage the tags available for assignment to the devices in your network. Tags can provide information such as the device's physical location and its administrator's email ID, and are used to group devices.

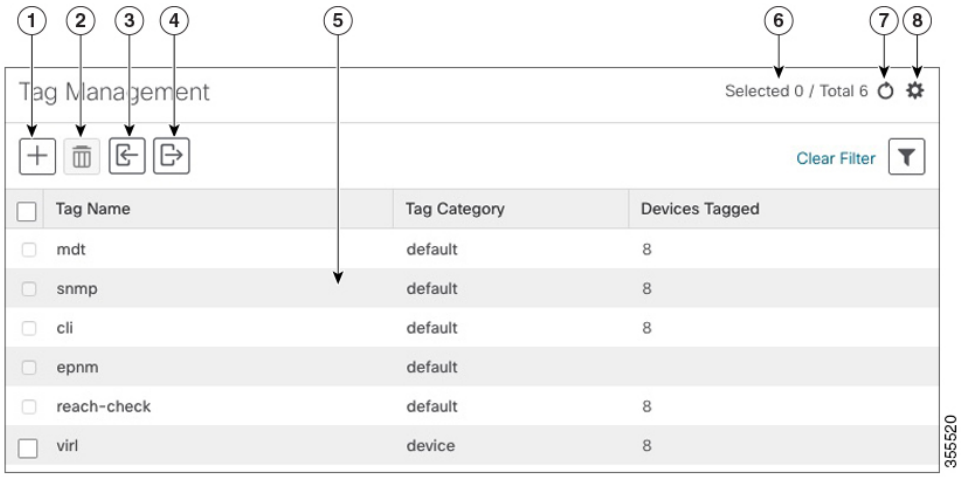
To open this window, choose **Administration** > **Tags**.

Note Cisco Crosswork applications automatically create a default set of tags and assign them to every device they manage:

- cli
- mdt
- reach-check
- snmp
- clock-drift-check

You cannot select, edit, delete, or manually associate these default tags with any device.

Figure 103: Tag Management Window



Item	Description
1	Click + to create new device tags. See Create Tags, on page 270.

Item	Description
2	Click to delete currently selected device tags. See Delete Tags, on page 272.
3	Click to import the device tags defined in a CSV file into the Cisco Crosswork application. See Import Tags, on page 271. 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. See Export Tags, on page 273.
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** window.
8	Click to choose the columns to make visible in the **Tag Management** window.
	Click to set filter criteria on one or more columns in the **Tag Management** window.
	Click the **Clear Filter** link to clear any filter criteria you may have set.

Create Tags

You can create as many tags and tag categories as you want. If you will have many tags, it might be quicker to list them in a CSV file and import the file, instead of creating each tag individually. See Import Tags, on page 271.

Note

- Tag and tag category names are case-insensitive and can contain a maximum of 128 alphanumeric characters, plus dots (.), underscores ("_") or hyphens ("-"). No other special characters are allowed.
- The maximum number of tags that you can create is 100.

Step 1 From the main menu, choose **Administration** > **Tags**. The **Tag Management** window opens.

Step 2 Click . The **Create New Tags** pane opens.

Step 3 In the **Category** area:

- To associate your new tags with an existing category: Choose the category from the drop-down list.
- To associate your new tags with a new category: Click the **New Category** link, enter the new category's name in the text field, and click **Save**.

All the new tags you create after this step will be assigned to the category you selected or created.

Step 4 In the **Tags** area: Start entering the names of the new tags that you want to create. Press **Return** after you type each tag.

To keep from entering duplicate tags, click the **Show Tags** link. The **Create New Tags** window will list only the tags that already exist in your currently selected category.

Step 5 When you are finished entering new tags, click **Save**.

What to do next

Add tags to devices. See Apply or Remove Device Tags, on page 272.

Import Tags

Complete the steps below to create a CSV file that lists the tags you want to apply to your devices, and then import it into the Cisco Crosswork applications. This is the easiest way to create a lot of new tags and tag categories quickly.

When you import the CSV file, any tags not already in the database will be added. Tags with the same name as an imported tag will be overwritten. For this reason, it is a good idea to export a backup copy of all your current tags before import (see Export Tags, on page 273).

Step 1 From the main menu, choose **Admin** > **Tags**.

Step 2 Click  to open the **Import CSV File** dialog box.

Step 3 If you have not already created a CSV file to import:

a) Click the **Download sample 'Tags 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 tag. Use a comma to delimit each field within a row. Use a semicolon to separate multiple entries in the same field.

Field	Description	Required or Optional
Tag Name	Enter the name of the tag. For example: `SanFrancisco` or `Spine/Leaf`.	Required
Tag Category	Enter 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 allowed.

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.

c) When you are finished, save the new CSV file.

Step 4 Click **Browse** to navigate to the CSV file you just created and then click **Open** to select it.

Step 5 With the CSV file selected, click **Import**.

The tags and tag categories that you imported should now be displayed in the **Tag Management** window.

What to do next

Add tags to devices. See Apply or Remove Device Tags, on page 272.

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.

In order to apply a tag to a device or group of devices, the tag must already exist. See Create Tags, on page 270 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.

You can apply a maximum of 15 tags to any one device.

To apply tags to a device or set of devices, do the following:

Step 1 From the main menu, 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 From the toolbar, click . The **Modify Tags** window opens, showing the tags currently applied to the device(s) you selected.

Step 5 Click in the **Type to autocomplete item** field to display the list of existing tags, or begin typing the name of the tag you want.

Step 6 Click on individual tags in the list to add them to the list of tags applied to the device(s). To delete an applied tag, click the X icon shown next to that tag.

Delete Tags

To delete device tags, do the following:

Note If the tag is mapped to any devices, then the tag cannot be deleted.

Step 1 Export a backup CSV file containing the tags you plan to delete (see Export Tags, on page 273).

Step 2 From the main menu, choose **Administration** > **Tags**. The **Tag Management** window is displayed.

Step 3 Check the check box next to the tags you want to delete.

Step 4 From the toolbar, click .

Step 5 The confirmation dialog box will list the number of devices currently using the tag(s) you are about to delete. Click **Delete** to confirm deletion.

Export Tags

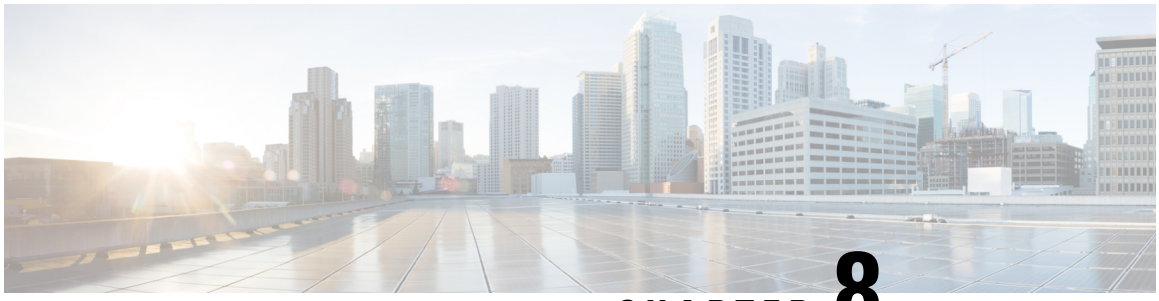
You can quickly export tags and tag categories to a CSV file. This will allow you to keep backup copies of your tags. You can also edit the CSV file as needed, and re-import it to overwrite existing tags. Note that you will need to re-associate devices and tags in some cases.

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

Step 2 (Optional) In the **Tag Management** window, filter the tag list as needed.

Step 3 Check the check boxes for the tags you want to export. Check the check box at the top of the column to select all the tags for export.

Step 4 Click . Depending on your browser, you will be prompted to select a path and file name to use when saving the CSV file, or to open it immediately.



CHAPTER 8

Onboard Devices

This section contains the following topics:

Add Devices to the Inventory

There are different ways to add devices to Crosswork. Each has its own set of prerequisites, which you must fulfill if the device addition is to succeed. Ensure that your devices are configured properly for communication and telemetry. See guidelines and example configurations in Configuration Prerequisites for New Devices, on page 276 and Sample Configuration for Cisco NSO Devices, on page 281.

In order of preference for most users, the methods and their prerequisites are:

1. **Importing devices using the Crosswork APIs:** : This is the fastest and most efficient of all the methods, but requires programming skills and API knowledge. For more, see the Inventory Management APIs On Cisco Devnet.
2. **Importing devices from a Devices CSV file**: This method can be time-consuming. To succeed with this method, you must first:
   - Create the provider(s) that will be associated with the devices. See About Adding Providers, on page 241.
   - Create corresponding credential profiles for all of the devices and providers listed in the CSV file. See Create Credential Profiles, on page 232.
   - Create tags for use in grouping the new devices. See Create Tags, on page 270.
   - Download the CSV template file from Crosswork and populate it with all the devices you will need.
3. **Adding them via the UI**: This method is the least error-prone of the three methods, as all data is validated during entry. It is also the most time-consuming, being suitable only for adding a few devices at a time. Note that the providers, credential profiles and tags you want to apply to them must exist beforehand. For more information, see Add Devices Through the User Interface, on page 282.

4. **Auto-onboarding from a Cisco SR-PCE provider**: This method is highly automated and relatively simple. Note that the device and provider credential profiles and tags you want to apply to these devices must exist beforehand. After onboarding devices from this source, you will need to edit each device to add device information that is not automatically discovered. For more information, see the provider properties in Add Cisco SR-PCE Providers, on page 249.
5. **Auto-onboarding using Zero Touch Provisioning**: This method is automated, but requires that you create device entries first and modify your installation's DHCP server. Note that the device and provider credential profiles and tags you want to apply to these devices must exist beforehand. After provisioning and onboarding devices using this method, you will need to edit each device to add information that is not automatically supplied. For more information, see the *Zero Touch Provisioning*chapter in the *Cisco Crosswork Network Controller 7.0 Device Lifecycle Management Guide*.

Note Cisco Crosswork only supports single-stack deployment modes. The devices can be onboarded with either an IPv4 address or an IPv6 address, not both.

If a device onboarded in Cisco Crosswork is on the same subnet as a Crosswork Data Gateway interface, then it must be on the data gateway's southbound network. This is because Crosswork Data Gateway implements Reverse Path Forwarding (RPF) checks and the source address of devices cannot be on the management or northbound networks if multitple NICs (2 or 3 NIC) are deployed.

Configuration Prerequisites for New Devices

Before onboarding new devices, ensure that the devices are properly configured in order to be managed by Cisco Crosswork Network Controller. The following sections provide sample configurations for several protocols, including SNMP, NETCONF, SSH, GNMI, Syslog, and TELNET. Use them as a guide to configuring the devices that you plan to manage.

Note

- SNMPv2 and SNMPv3 (Auth/Priv) traps are supported.
- The SNMP EngineID generated or configured in the device should be unique in the network.
- For the credentials to work, SNMP users should be re-created if the SNMP EngineID is re-configured in the device.
- In the sample configurations, *cdg_virtualIP* denotes the virtual IP address of the data gateway in a data gateway pool. The *cdg_virtualIP* varies for each pool.
- When devices are onboarded with *Sys Object ID* contact the Cisco Customer Experience team as the platform may not be certified by Cisco.

Configure Devices to Forward Events to Crosswork Network Controller

To ensure that Crosswork Network Controller can receive events and notifications from devices, configure the devices to forward events to the Crosswork server. 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.

Note In the event of a failover, the standby data gateway within the same data gateway pool automatically inherits the virtual IP address of the active data gateway. You do not require any additional configuration, allowing for a simplified and efficient failover strategy.

We recommend using a common configuration file for all your devices to allow Crosswork to perform a reachability check and collect trap information.

The ZTP users need to define the events they want the device to send to Crosswork in the pre-configuration, day-zero, or post-configuration files. Non-ZTP users should establish which events the device must send to Crosswork and decide on the method of communication for these events.

For example, you can configure a device to forward events to the Crosswork 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 traps snmp linkup
snmp-server traps snmp linkdown
```

To set the SNMP view:

```
snmp-server view { group name } include
```

Confiure Devices for Pre-Onboarding Tasks

The following commands provide a sample pre-onboarding device configuration that sets the correct SNMPv2 and NETCONF configuration, and SSH and Telnet rate limits. The NETCONF setting is only needed if the device is MDT-capable.

Note Ensure that you set the snmp-server packetsize to 4096 to avoid getting duplicate packets and "unable to acquire feed" errors.

```
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
snmp-server packetsize 4096
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 SNMPv3 Devices

If you want to enable SNMPv3 data collection, repeat the SNMPv2 configuration commands in the previous section, and add the following commands:

```
snmp-server group grpauthpriv v3 priv notify v1default
snmp-server user <user-ID> grpauthpriv v3 auth md5 password priv aes 128 password
```

Configure SNMPv2 and SNMPv3 Traps

To configure the device to send SNMP traps, use the following commands:

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
```

Note that, for traps to be received, the node_ip field for the device as listed in the Cisco Crosswork inventory must match the IP address of the device interface from which the traps are sent. If they do not, Cisco Crosswork will reject the traps. Also, the device needs to be in ADMIN_UP state for traps to be received.

Configure Required Settings for Cisco IOS XR Device Operating System

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 ssh
transport output ssh
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 for alarm and event management. NTP settings ensure that Crosswork 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
```

Enable performance management on all optical data unit (ODU) controllers:

```
controller oduX R/S/I/P
per-mon enable
```

Configure Required Settings for Cisco IOS and IOS-XE Device Operating System

```
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 ssh (requird only if ssh is used)
transport output ssh (required only if ssh isused)
```

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 Crosswork for alarm and event management. NTP settings ensure that Crosswork 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]
```

Sample Configuration for Cisco NSO Devices

When using Cisco Network Services Orchestrator (Cisco NSO) as a provider to configure devices managed by Cisco Crosswork, make sure that the Cisco NSO device configurations observe the guidelines in the following example.

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
```

Add Devices Through the User Interface

Follow the steps below to add devices one by one, using the user interface. This method is mostly used when adding a few devices only.

Step 1 From the main menu, choose **Device Management** > **Network Devices**.

Step 2 Click  .

Step 3 Enter the values for the new device, as listed in the table below.

Step 4 Click **Save**. The Save button is disabled until all mandatory fields are completed.

Step 5 (Optional) Repeat these steps to add more devices.

Table 23: Add New Device Window (*=Required)

Field	Description
*** 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**.
*** Credential Profile**	The name of the credential profile to be used to access the device for data collection and configuration changes. For example: **nso23** or **srpce123**. This field is optional if **Configured State** is marked as **UNMANAGED**.
Host Name	The hostname of the device.
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.
Software Type	Software type of the device.
Software Version	Software version of the operating system.

Field	Description
UUID	Universally unique identifier (UUID) for the device.
Serial Number	Serial number for the device.
MAC Address	MAC address of the device.
*** 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**.
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.
Product Type	Product type of the device.
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, on page 106 for more details
Connectivity Details	
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 + at the end of the first row in the **Connectivity Details** panel. To delete a protocol you have entered, click × 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. You must 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** 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. **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.
*** Port**	The port used for this connectivity protocol. Each protocol is mapped to a port, so be sure to enter the port number that corresponds to the protocol you chose. The standard port assignments for each protocol are: • SSH: 22 • SNMP: 161 • NETCONF: 830 • TELNET: 23 • HTTP: 80 • HTTPS: 443 GNMI and GNMI_SECURE: 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 will time out. The default value is 30 seconds. For XE devices using NETCONF, the recommended minimum timeout value is 90 seconds. 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 only applicable for **SNMP** protocol. From the drop-down list, select the relevant SNPMv3 protocol supported by the device. The default value is NONE. The drop-down menu lists Advanced Encryption Standard (AES) specifications in Counter mode (CTR), Galois/Counter mode (GCM), and Cipher Block Chaining mode (CBC) for different key lengths (128-bit, 192 bit, 256 bit). The credential profile supports generic privacy types such as AES-192 and AES-256. For Cisco devices, AES-192 and AES-256 are customized as CiscoAES192 and CiscoAES256 protocols. On the devices, these protocols are displayed as aes256-ctr, aes256-gcm@openssh.com, aes256-cbc, aes192-ctr, and aes192-cbc. The Cisco devices will only respond to Crosswork Network Controller's polling if it is based on the new protocol variations. For devices other than Cisco, select None in the **Encryption** field.

Field	Description
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.
Routing Info	
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.
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.
***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 in the device type. This field is optional. **Note** This field can be edited only when the device is in 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 needs to 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.	
Longitude, **Latitude**	Longitude and latitude values are required so that the geographical map can present the correct geographical location of the device and its links to other devices. Enter the longitude and latitude in Decimal Degrees (DD) format.
Altitude	The altitude at which the device is located. For example, **123**.
Providers and Access To add more providers for this device, click + at the end of the first row in the **Providers and Access** panel. To delete a provider you have entered, click × shown next to that row in the panel.	
Provider Family	Provider type used for topology computation. Choose a provider from the list.

Field	Description
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.

Add Devices by Importing from CSV File

Complete the steps below to create a CSV file that specifies multiple devices and then import it into Crosswork Network Controller. This allows you to add multiple devices at once instead of adding each device individually.

Importing devices from a CSV file adds any devices not already in the database, and overwrites the data in any device record with an Inventory Key Type field value that matches those of an imported device (this excludes the UUID, which is set by the system and not affected by import). For this reason, it is a good idea to export a backup copy of all your current devices before an import.

Note Importing devices using CSV or API methods will fail if the CSV file contains data gateway information. To successfully import the devices, ensure that the Crosswork Data Gateway and UUID columns in the CSV file are empty before you proceed.

Step 1 From the main menu, choose **Device Management** > **Network Devices**. The **Network Devices** tab is displayed by default.

Step 2 Click  to 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.

Note
- Ensure that the TE router ID value for each device is populated. This value uniquely identifies the device within the topology as provided by SR-PCE.
- The CSV files created on a Windows machine should contain a new line (marked with a 'newline' character) for the file to be processed as expected. Any newline created using the "carriage return" option will not work.

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

For a list of the fields and the mandatory values you must enter, see the "Add New Device" field table in Add Devices Through the User Interface, on page 282.

c) Delete the sample data rows before saving the file, or they will be imported along with your data. The column header row can stay, as it is ignored during import.

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.

It is normal for devices to 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.

Step 7 Once you have successfully onboarded the devices, you must map them to a data gateway instance.

Export Device Information to a CSV File

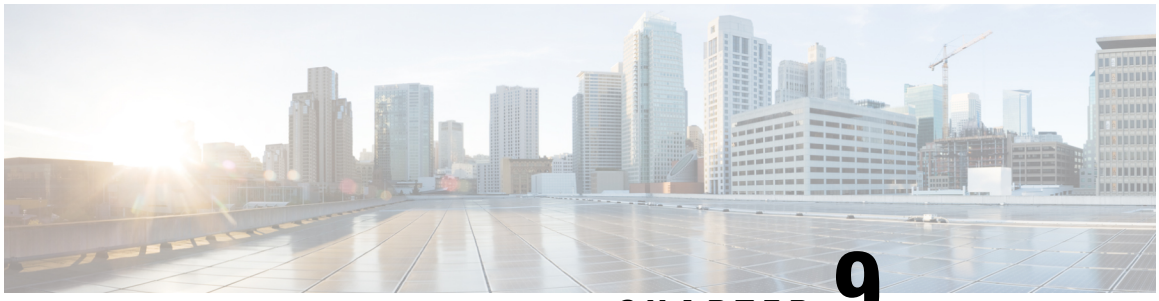
Exporting the device list is a handy way to keep a record of all devices in the system at one time. You can also edit the CSV file as needed, and re-import it to overwrite existing device data.

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  . Your browser will prompt you to select a path and the file name to use when saving the CSV file, or to open it immediately.



CHAPTER 9

Manage System Access and Security

This section contains the following topics:

Manage Certificates

What is a Certificate?

A certificate is an electronic document that identifies an individual, a server, a company, or another entity, and associates that entity with a public key. 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. A certificate is signed by an issuer or a "parent" certificate (Certificate Authority) - i.e. signed by the parent's private key. Certificates can also be self-signed. 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. Starting from the root certificate's private key, the private key for each certificate in the trust chain signs and issues the next certificate in the chain until finally signing an end entity certificate. The end-entity certificate is the last certificate in the chain and is used as a client or server certificate. For more details about these protocols, see X.509 Certificates, on page 359 and HTTPS, on page 359.

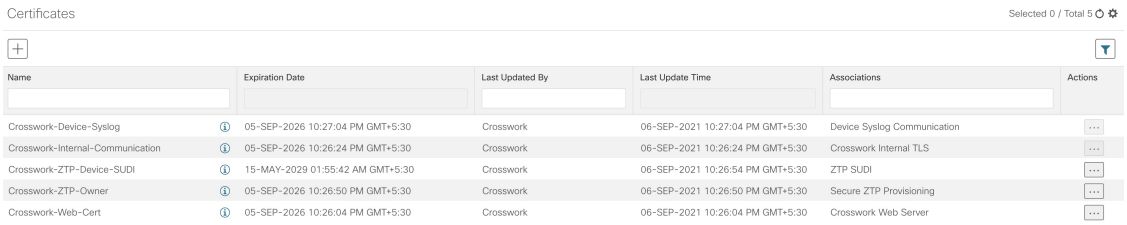
How are Certificates Used in Crosswork?

Communication between Crosswork applications and devices as well as between various Crosswork 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 uses a mix of generated and client uploaded certificates. Uploaded certificates can be purchased from Certificate authorities (CA) or can be self-signed.

For example, the Cisco Crosswork VM-hosted web server and the client browser-based user interface communicate with each other using Crosswork generated X.509 certificates exchanged over TLS.

The Crosswork Cert Manager is a proxy for multiple microservices and services within the distributed framework and manages all the Crosswork certificates. The Certificate Management UI (**Administration** > **Certificate Management**) allows you to view, upload, and modify certificates. The following figure displays the default certificates provided by Cisco Crosswork.

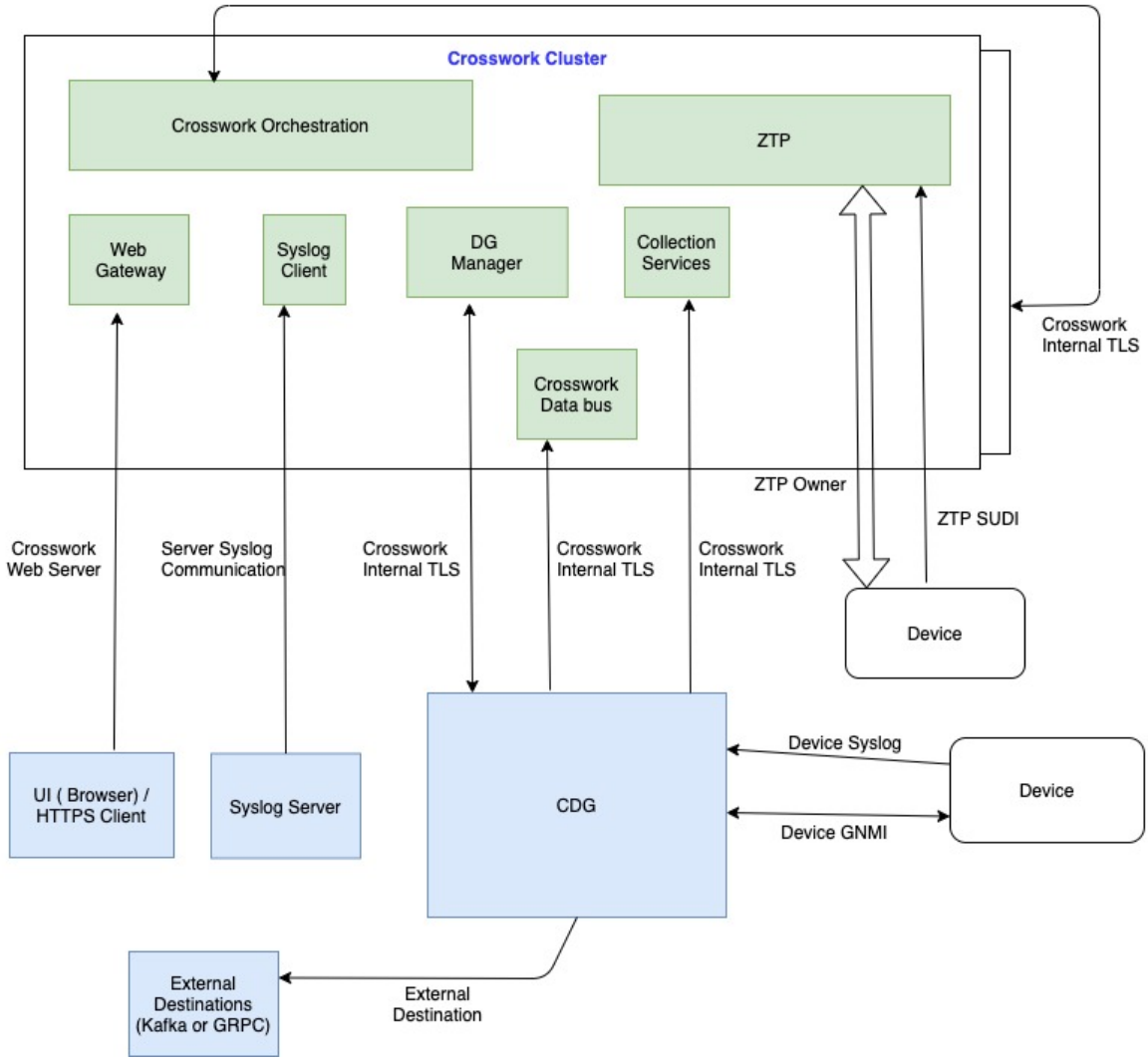
Figure 104: Certificate Management UI



Certificate Types and Usage

The following figure shows how Crosswork uses certificates for various communication channels.

Figure 105: Certificates in Cisco Crosswork



These certificates are classified into various roles with different properties depending on their use case as shown in the following table.

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Crosswork (CW) Internal TLS	CW-Internal-Communication	• Generated and provided by Crosswork. • This trust-chain is available in the UI (including the server and client leaf certificates) and is created by Crosswork during initialization. They are used for interprocess communications between Crosswork and Crosswork Data Gateway and communication between internal Crosswork components. • Allows mutual and server authentication.	Crosswork	• Crosswork Data Gateway • Crosswork	Download	5 years	—
CW Web Server	CW-Web-Certificate Server Authentication	• Generated and provided by Crosswork. • Provides communication between the user browser and Crosswork. • Allows server authentication.	Crosswork Web Server	User Browser or API Client	• Upload • Download	5 years	30 days to 5 years

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
ZTP SUDI	CW-ZTP-Device-SUDI	• A public Cisco certificate that is provided as part of Crosswork. • Provides ZTP protocol communication channel between the ZTP application and device. • Allows server authentication.	Crosswork ZTP	Device	• Upload • Download	100 days	30 days. This value is user-defined
Secure ZTP Provisioning	CW-ZTP-Owner	• Generated and provided by Crosswork. • Forwarded by ZTP to devices and used for second layer of encryption.	Crosswork ZTP	Device	• Upload • Download	5	30 days. This value is user-defined
Device Syslog	CW-Device-Syslog	• Generated and provided by Crosswork. • Provides Syslog telemetry communications between devices and Crosswork Data Gateway. • Allows server authentication.	Crosswork Data Gateway	Device	Download	5 years	—
Device gNMI Communication	—	Provides GNMI telemetry communications between devices and Crosswork Data Gateway.	Crosswork Data Gateway	Device	• Upload • Download	Not Applicable	30 days. This value is user-defined

Role	UI Name	Description	Server	Client	Allowed operations	Default Expiry	Allowed Expiry
Server Syslog Communication	—	• Allows syslog events and logs from Crosswork to an external Syslog server. • Allows server authentication.	External Syslog Server	Crosswork	• Upload You can upload multiple certificates associated with different servers. • Download	—	30 days. This value is user-defined
External Destination	—	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a mutual-authentication.	External Destinations (Kafka or gRPC)	Crosswork Data Gateway	• Upload [1] • Download	—	30 days. This value is user-defined
External Destination Server Auth	—	Exports telemetry data from Crosswork Data Gateway to external destinations (Kafka or gRPC) after performing a server-based authentication.	External Crosswork Data Gateway Destinations (Kafka or gRPC)	Crosswork Data Gateway	• Upload [2] • Download	—	30 days. This value is user-defined
Secure LDAP Communication	—	Crosswork uses the trust chain of this certificate to authenticate the secure LDAP server.	Secure LDAP server	Crosswork	• Upload • Download	—	30 days. This value is user-defined
Application External Destination	—	Exports telemetry data from Crosswork to an external Kafka destination.	External Kafka Destinations	Crosswork	Upload	—	30 days. This value is user-defined

[1] You can upload multiple certificates associated with different destinations.

[2] You can upload multiple certificates associated with different destinations.

There are two category roles in Crosswork:

- 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

You can add certificates for the following 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, the user uploads 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 any number of optional intermediate CA certificates. The last intermediate certificate in the chain and its corresponding private key is uploaded separately in the UI using **Intermediate key**, **Intermediate certificate**, and optionally **Passphrase** (if one was used for generating the intermediate key). Crosswork internally creates a client certificate using this intermediate key for the Crosswork Data Gateways that connects to the external destination. The destination (for example: Kafka) server certificate trust needs to 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 78.

- **Server Syslog Communication**: The user uploads the trust chain of the Syslog server certificate. This trust chain is used by Crosswork to authenticate the Syslog server. Once this trust chain is uploaded and propagated within Crosswork, the user 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, on page 362.

- **Devices gNMI communication**: The user uploads 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 Configure gNMI Certificate, on page 119.

- **Secure LDAP Communication**: The user uploads 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, the user can add the LDAP server (see Manage LDAP Servers, on page 349) and associate the certificate.

- **External Destination Server Auth**: The user uploads the root CA certificate. This certificate is used to establish a secure communication between Crosswork Data Gateway and external destinations like Kafka servers.

  You can upload the certificates to the **External Destination Server Auth** role only when the authentication type is set to **Server-Auth**. For more information about the authentication types, see Add or Edit a Data Destination, on page 78.

- **Application External Destination**: The user can upload the application certificates to ensure secure transfer of telemetry data to an external Kafka destination. The Kafka channel is safeguarded through mutual TLS, and the TLS Manager is responsible for managing the certificates used by external Kafka.

Note Cisco Crosswork 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 Cisco Crosswork), use the Edit function (see Edit Certificates, on page 296).

Before you begin

- For information on certificate types and usage, see Certificate Types and Usage, on page 290.
- All certificates that are uploaded must be in Privacy Enhanced Mail (PEM) format. Note where these certificates are in the system so that you can navigate to them easily.
- Trust chain files that are uploaded 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.
- Intermediate Keys need to be either PKCS1 or PKCS8 format.
- A data destination must be configured prior to adding a new certificate for an external destination. For more information, see Add or Edit a Data Destination, on page 78.
- Ensure there are no collection jobs configured for destinations when adding or updating a certificate with multiple destinations.

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 menu, select the purpose for which the certificate is to be used. For more information, see Certificate Types and Usage, on page 290.

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 Once uploaded, the Crosswork Cert manager accepts, validates, 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.

Edit Certificates

You can edit a certificate to add or remove connection destinations, upload, and replace expired or misconfigured certificates. User provided certificates, ZTP certificates, and web certificates can be edited. Other system certificates that are provided by Cisco Crosswork cannot be modified and will not be available for selection.

You can also “remove” a certificate by following this procedure to replace the certificate or by disabling security (disable **Enable Secure Communication** option) for any assigned destinations (see Add or Edit a

Data Destination, on page 78). Permanently deleting a certificate from the Cisco Crosswork system is not supported.

Step 1 From the main menu, choose **Administration** > **Certificate Management**. and check the certificate that you want to modify.

Step 2 Click ⋯ on the certificate that you want to modify and select **Update Certificate**.

Step 3 Update the necessary options.

Note While updating a CW Web Server Certificate, provide relevant values for the following fields:

- **Crosswork Web CA**: Trust chain file (in PEM format) containing the root CA certificate and zero or more intermediate certificates.
- **Crosswork Web Intermediate**: An intermediate CA certificate signed with the root CA certificate.
- **Crosswork Web Intermediate Key**: The key associated with the intermediate CA certificate.
- **Crosswork Web Passphrase**: This is an optional field.

Upon successful validation, the Certificate Management UI logs out automatically and applies the certificate to the Web Gateway.

Step 4 Click **Save**.

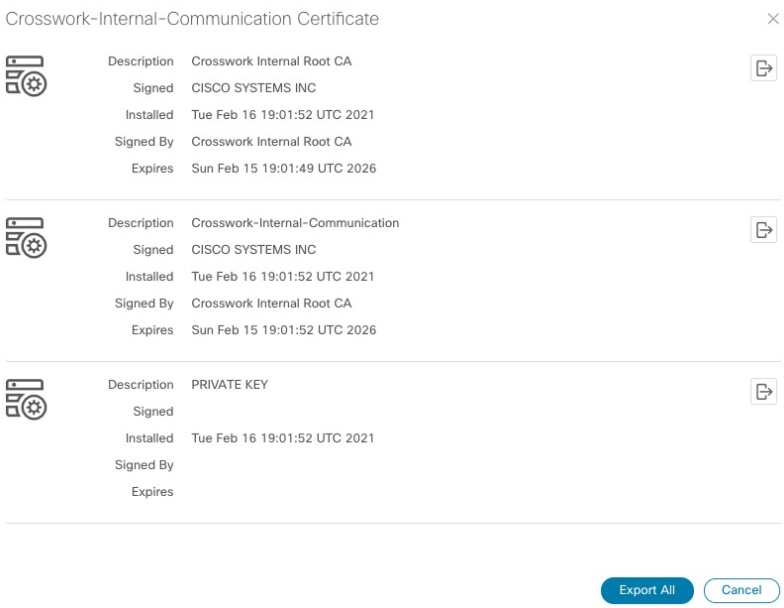
Download Certificates

To export certificates, do the following:

Step 1 From the main menu, choose **Administration** > **Certificate Management**.

Step 2 Click ⓘ for the certificate you want to download.

Figure 106: Export Certificates



Step 3 To separately download the root certificate, intermediate certificate, and the private key, click . To download the certificates and private key all at once, click **Export All**.

Renew Certificates

Kubernetes Certificate Renewal

Certificates are valid for one year before they expire. After renewing the certificates, ensure that the pods are healthy before resuming other operations.

Note When renewing certificates before expiry, it is recommended to perform this activity during a maintenance window as the cluster is in an operational state.

To renew a certificate, perform the following:

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.

Step 1 Create a backup of your Crosswork Network Controller.

Step 2 Log in to one of your hybrid nodes.

Step 3 Run the following command:

Attention The command below has line breaks inserted for display purposes. Please remove these line breaks before executing it.

```
renew_k8s_cert --hybrid=hybridNodeMgmtIP1,hybridNodeMgmtIP2,hybridNodeMgmtIP3
--worker=workerNodeMgmtIP1,workerNodeMgmtIP2,workerNodeMgmtIP3 --user=<ssh-username>
--passwdfile=<passfile-path>
```

Replace the parameters with the management IP addresses of the nodes in your cluster.

- `hybridNodeMgmtIP`: Management IP of the hybrid node.
- `workerNodeMgmtIP`: Management IP of the worker node. You can add this parameter according to the number of worker nodes in your cluster. If no worker nodes are available, you can skip this parameter.
- `ssh-username`: The SSH username
- `passfile-path`: The path for the plain text file that contains the SSH login password.

Here are some examples:

- 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
  ```

- Example for a 3-node cluster:

  ```
  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
  ```

- Example for the single VM deployment:

  ```
  renew_k8s_cert --hybrid=10.10.10.101  --user=cw-admin --passwdfile=/home/cw-admin/password.txt
  ```

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 2 years will face certificate expiry, disrupting TLS communication and impacting 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 60 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:**

- In the case of a Geo HA deployment, the certificate renewal is triggered in the active AZ cluster. Internally, 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. Once the renewal job is completed on the active cluster, the job will automatically run in the standby cluster after a delay of a few minutes. The job progress is displayed on the standby cluster along with alarm events.

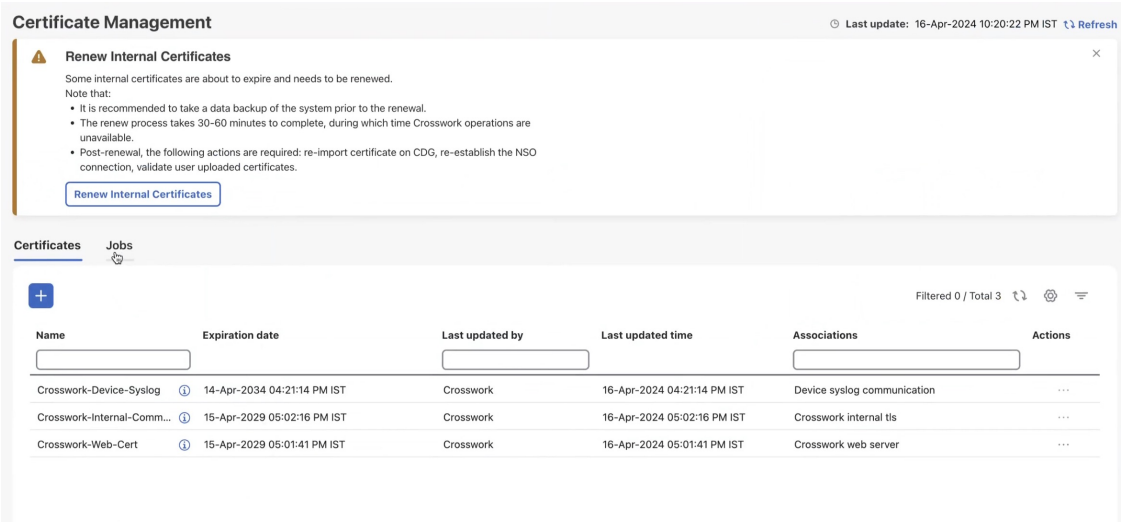
The certificate renewal process can cause a downtime of approximately 30 minutes to 1 hour. It is recommended to perform this activity during a maintenance window to avoid disrupting cluster operations.

To renew an internal certificate, perform the following:

Step 1 From the main menu, choose **Administration** > **Certificate Management**. The **Certificate Management** window is displayed. If an internal certificate is about to be expired, a prompt is displayed for certificate renewal.

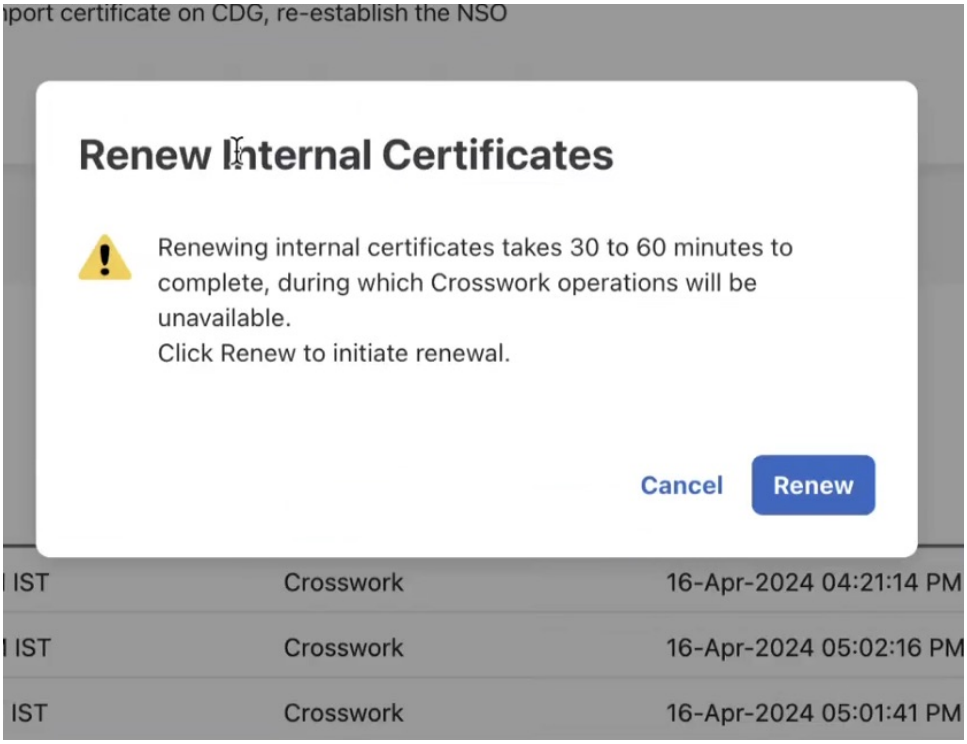
Note Alerts about certificate expiry are displayed on the Crosswork dashboard when you log in. These alerts will be generated at various stages of the certificate expiry, with increasing severity as the expiry date approaches.

Figure 107: Renew Internal Certificate prompt



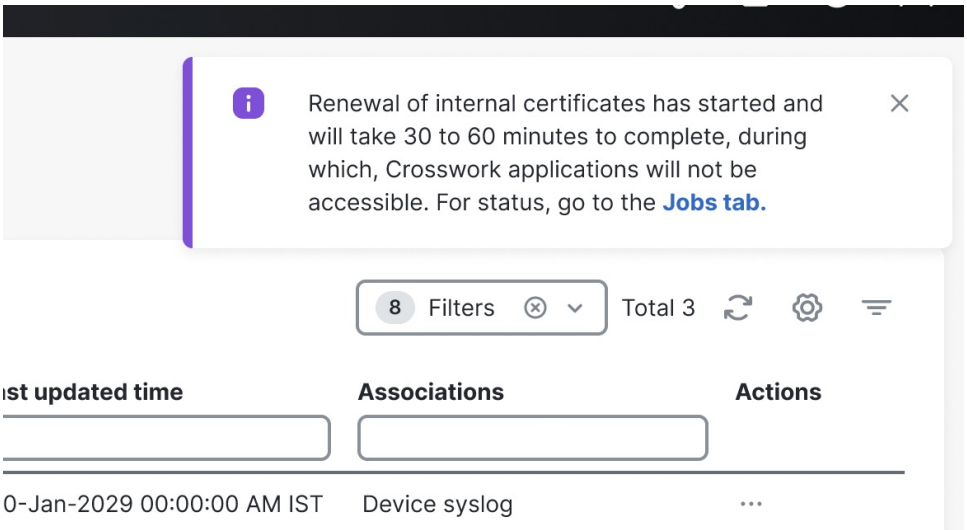
Step 2 Click **Renew Internal Certificate**. A confirmation popup is displayed. Click **Renew** to confirm.

Figure 108: Renewal Confirmation Prompt



This action invokes the REST API (/v2/cert/renew) and initiates the certificate expiry check. A notification about the new renewal job is displayed on the **Certificate Management** window.

Figure 109: Renewal Job Notification



You can view progress of the renewal job from the **Jobs** tab. Once the job is complete, an Info alarm event is raised about the successful completion. 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 as the API is idempotent.

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 Once the renewal job is completed, perform the following steps to ensure TLS communication is maintained between Crosswork and other external components:

a) **Crosswork with Crosswork Data Gateway**: Re-import the newly recreated `controller.pem` signing certificate on Crosswork Data Gateway as `dg-admin` user. For more information, see Import Certificate, on page 402. This action prevents the deletion of Data Gateway instances, avoids the detachment and re-attachment of devices, and ensures the continuation of collection and other offload operations.

Note This action is also performed as part of the Crosswork Data Gateway day-N enablement as well.

b) **Crosswork Data Gateway - Device Syslog**: If device syslog root and intermediate certificates are renewed, users must 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 Job, on page 105.

if there is a renewal for device syslog root and intermediate certificates, users must manually export these certificates to the devices.

c) **External destination/Server Auth CA**: Re-upload the External Destination and Server Auth CA certificates to Crosswork.

d) **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 Configure Standalone NSO, on page 336 section.

Manage Licenses

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 across your organization. And it's secure – you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** My Cisco Entitlements (MCE) provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.
- **License Flexibility:** Your software is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco Software Central (software.cisco.com). A **Cisco Smart Account** provides the repository for Smart enabled products and enables you to activate Cisco licenses, monitor license usage and track Cisco purchases. The **Cisco Smart Software Manager (CSSM)** enables you to manage all your Cisco Smart software licenses from one centralized website. With Cisco Smart Software Manager, you may create and manage multiple virtual accounts within your Smart Account to manage licenses. For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide.

From the main menu, select **Administration** > **Smart Licenses** to display the **Smart License** tab under the **Application Management** window. In the **Smart License** tab, you can register your Crosswork Network Controller application, edit the transport settings, renew the license, and de-register your application.

Important All unmanaged devices are counted towards the device limits associated with Crosswork licenses. To prevent this, delete your unmanaged devices in the Crosswork UI.

Note Licenses for lab systems are obtained through the same process as those for production environments. If you require a license for a lab beyond the 90-day trial period, please coordinate with your account team or a Cisco partner to have the appropriate license issued.

Tracked Node Counts for Crosswork Optimization Engine

For Crosswork Optimization Engine, the node count is reported in the following cases:

- After initial installation and startup of the following pods: Crosswork UI, RESTCONF, or any of the feature packs (Local Congestion Mitigation, Bandwidth on Demand, or Circuit Style Manager).
- Manually restarting the pods
- Daily at a fixed time (1:00 AM)

Configure Transport Settings

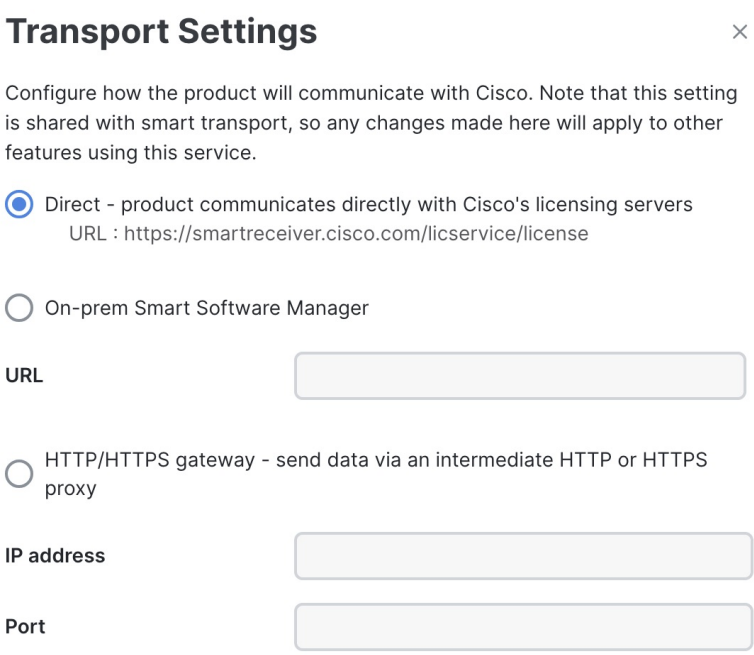
You can configure the transport settings to decide how Crosswork Network Controller communicates with the Cisco servers.

Note Transport Settings cannot be changed while the Crosswork product is in Registered mode. You have to de-register to change them.

Step 1 In the **Smart License** tab, the Transport Settings display the current transport mode selected. To modify, click **View/Edit**.

The **Transport Settings** dialog box is displayed.

Figure 110: Transport Settings Dialog Box



Step 2 Select the relevant transport mode and make relevant entries in the fields provided.

- **Direct**: The application directly connects with Cisco Smart Software Manager (CSSM).
- **On-prem Smart Software Manager**: The application communicates via CSSM On-Prem, ensuring that all user communication remains on premises. For more information on the CSSM on-prem option, see the Smart Software Manager guide.
- **HTTP/HTTPS Gateway**: The application connects via an intermediate proxy server. This is applicable only for Direct mode.

Step 3 Click **Save**.

Register Crosswork Network Controller Application

To enable licensed features, the Crosswork Network Controller application must be registered to CSSM using a registration ID token or a reserved license. Once registered, an Identity Certificate is saved securely 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.

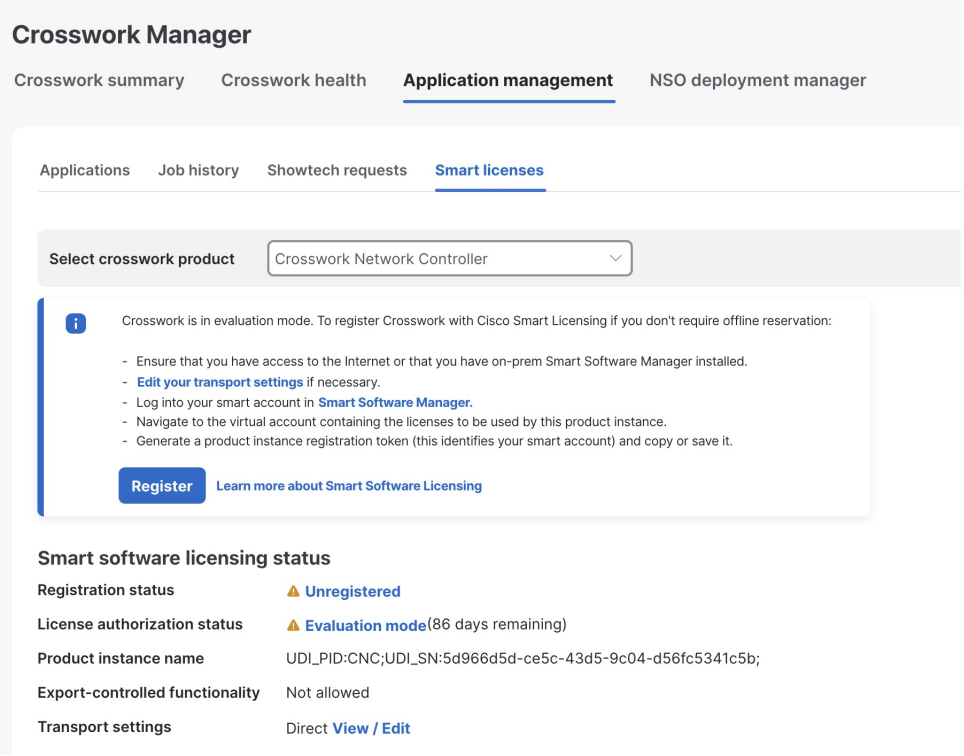
Note For information on generating the registration token, please refer to the support resources provided in the Smart Software Manager webpage.

Crosswork also supports registration of solution-based entitlements for Crosswork.

Step 1 From the main menu, select **Administration** > **Smart Licenses** to display the **Smart Licenses** tab.

The registration status and license authorization status will be **Unregistered** and **Evaluation mode** respectively.

Figure 111: Smart Software Licensing Unregistered Example



Step 2 Click the **Select Crosswork Product** drop-down list and select your product. In you plan to register a specific application, select the application from the list.

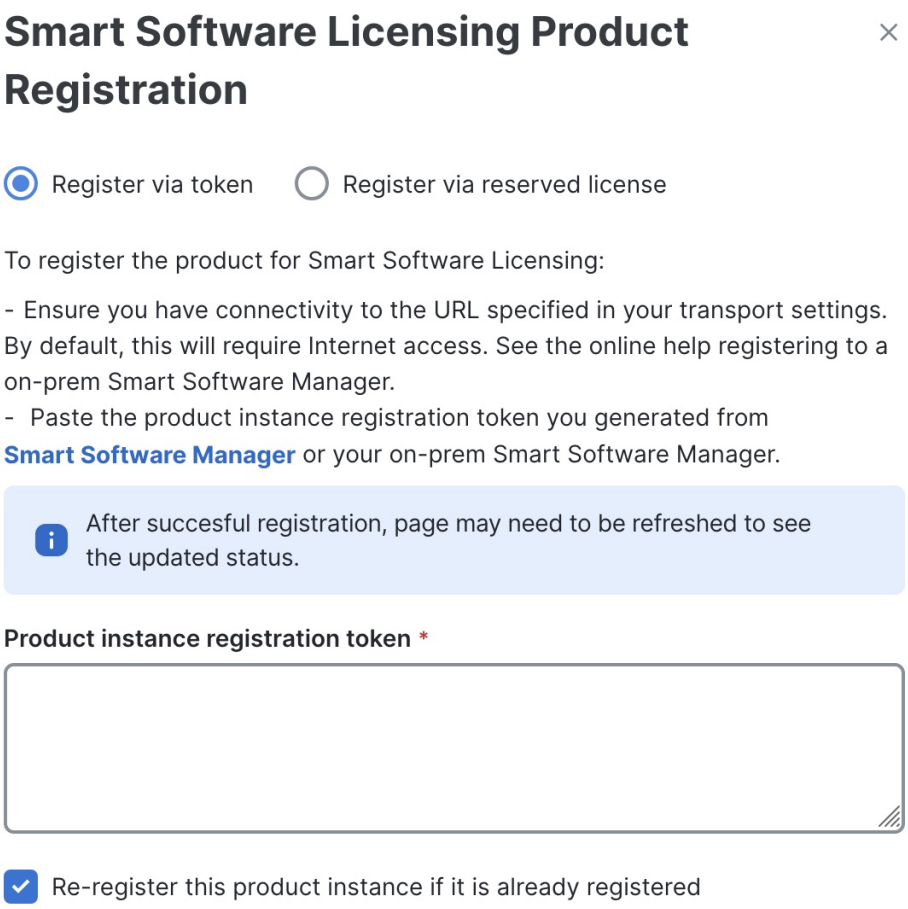
- If you plan to register using a solution-based license, select **Crosswork Network Controller**.
- In you plan to register a specific application, select the application name from the list.

Important You can register an application using either a solution-based license or an application-specific license, but not both. If you attempt to register a product that is already licensed, the system will display an error and prompt you to deregister the previous license. Depending on the type of licensing you choose (solution-based or application-based), the respective entitlements will be displayed.

Step 3 In the **Smart Software Licensing** dialog box, click **Register**.

The Smart Software Licensing Product Registration dialog box is displayed. The **Register via token** radio button is selected by default.

Figure 112: Smart Software Licensing Product Registration Dialog Box



Step 4 In the **Product Instance Registration Token** field, enter the registration token generated from your Smart Account. Make sure the token ID is accurate and within validity period. For more information, see https://www.cisco.com/c/en_in/products/software/smart-accounts/software-licensing.html.

Step 5 (Optional) If you are re-registering the application, check the **Re-register this product registration if it is already registered** check box.

Note After a backup restore, disaster recovery, or data migration operation, you must manually re-register the Cisco Crosswork VM to CSSM. This applies if the Cisco Crosswork VM was already registered at the time the backup was taken and is used in the restore operations.

Step 6 Click **Register**. It may take a few minutes to process the registration. If successful, the 'Product Registration completed successfully' message is displayed.

The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

Note

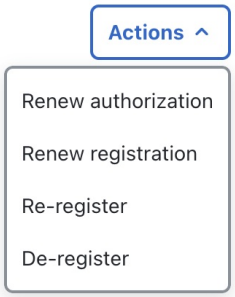
- If you encounter a registration error (e.g., *"Communication send error"* or *"Invalid response from licensing cloud"*), please wait for some time and retry the registration. If the error persists after multiple attempts, please contact the Cisco Customer Experience team for assistance.
- If you encounter 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, you may need to manually refresh the page to see the updated status.

Manually Perform Licensing Actions

The renewal of registration and authorization are automatically enabled for Crosswork Network Controller, by default. However, in the event of a communication failure between the application and the Cisco server, these actions can be manually initiated. You can use the **Actions** drop-down button to manually renew, re-register and de-register the application.

Step 1 In the **Smart License** tab, click **Actions** drop-down button and select the relevant option for the following quick actions.

Figure 113: Actions drop-down menu



a) **Actions** > **Renew Authorization**: To renew the authorization manually if the automatic renewal service fails at the end of 30 days.
b) **Actions** > **Renew Registration**: To renew the registration manually if the automatic renewal service fails at the end of 6 months.
c) **Actions** > **Re-register**: Re-register the application, for example, on account of the expiry of registration tokens.
d) **Actions** > **De-register**: De-register the application, for example, when the transport settings need to be changed.

Note Once de-registered, the application will be moved to **Evaluation** mode (if evaluation period is available), or **Evaluation Expired** mode. For more information, see License Authorization Statuses, on page 310.

Step 2 The selected action is executed successfully.

Register Cisco Crosswork Applications via Offline Reservation

Cisco Crosswork applications that use Smart Licensing share 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.

There are two modes of offline reservation:

- Specific License Reservation (SLR)—In this mode, you can select the number of licenses of each entitlement that has to be reserved.
- Permanent License Reservation (PLR)—In this mode, there will be a single license that will make the entire product In Compliance.

Before you begin

Confirm that you have a Smart Account. If not, go to Smart Account Request and follow the instructions on the website.

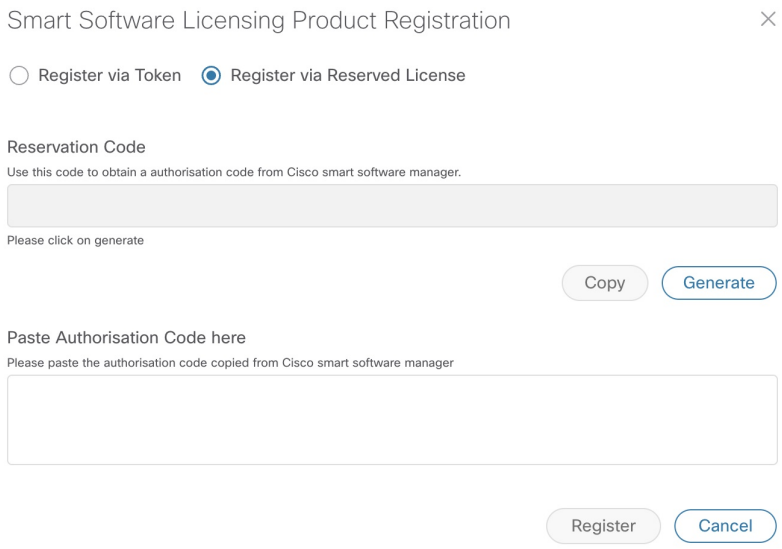
Step 1 From the main menu, select **Administration** > **Smart Licenses** to display the **Smart License** tab.

Step 2 Click **Register**.

The Smart Software Licensing Product Registration dialog box is displayed.

Step 3 Select the **Register via Reserved License** option.

Figure 114: Smart Software Licensing Product Registration Dialog Box



Step 4 Click the **Generate** button under the Reservation Code section. Your Reservation Request Code is generated and populated in the text field. Copy this code using **Copy** button.

Step 5 Go to the Cisco Software Central website and select the appropriate virtual account.

Step 6 Click the **Licenses** tab, then click **License Reservation**. Paste the Reservation Request Code that you generated in Step 4 and click **Next**.

Step 7 In the Select Licenses page, select the **Reserve a specific license** radio button, reserve the necessary licenses from the list, and click **Next**.

Step 8 In the Review and Confirm page, click **Generate Authorization Code**. Copy the code using the **Copy to Clipboard** button.

Step 9 Navigate back to the Smart Software Licensing Product Registration page on the Cisco Crosswork UI. Paste the Authorization Code in the text field under the **Paste Authorisation Code here** section.

Step 10 Click **Register**. It may take a few minutes to process the registration.

The registration status and license authorization status will be updated as **Registered** and **Authorized** respectively.

Update Offline Reservation

Use the **Update Reservation** option to update the license counts reserved via offline reservation.

Step 1 From the main menu, select **Administration** > **Smart Licenses** to display the **Smart License** tab. Make a note of the Product Instance Name (available under the Smart Software Licensing Status section).

Step 2 Go to the Cisco Software Central website and select the appropriate virtual account.

Step 3 Click the name of the product instance that matches your Product Instance Name.

Step 4 Click the **Actions** drop-down button and choose **Update Reservation**.

Step 5 In the Select Licenses page, select the **Reserve a specific license** radio button, update the count of the necessary licenses from the list and click **Next**.

Step 6 In the Review and Confirm page, click **Generate Authorization Code**. Copy the code using **Copy to Clipboard** button.

Step 7 Navigate back to the Smart License page on the Cisco Crosswork UI. Click the **Actions** drop-down button and choose **Update Reservation**. Paste the Authorization Code that you generated in Step 6 and click **Update**.

A Confirmation Code is generated. You can find this under the Smart Software Licensing Status section. Copy this code.

Step 8 Navigate back to the Cisco Software Central website. Click the required product instance name.

Step 9 Click the **Actions** drop-down button and choose **Enter Confirmation Code**.

Step 10 Enter/paste the Reservation Confirmation Code that was generated in Step 7 and click **OK**.

The license count will be updated on the Smart License page of the Cisco Crosswork UI.

Disable Offline Reservation

Use the **Disable Reservation** option 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. For more information, see License Authorization Statuses, on page 310.

Step 1 From the main menu, select **Administration** > **Smart Licenses** to display the **Smart License** tab. Make a note of the Product Instance Name (available under the Smart Software Licensing Status section).

Step 2 Click the **Actions** drop-down button and choose **Disable Reservation**.

Step 3 In the Confirm Disable Reservation window, click **Confirm**.

A Release Code (Reservation Return Code) is generated. Copy this code using the **Copy** button.

Step 4 Navigate to the Cisco Software Central website and select the appropriate virtual account.

Step 5 Click the name of the product instance that matches your Product Instance Name.

Step 6 Click the **Actions** drop-down button and choose **Remove**.

Step 7 In the Remove Reservation pop-up, paste the Reservation Return Code that you generated in Step 3 and click **Remove Reservation**.

The Registration Status will be updated to Un Rgistered state on the Smart License page of the Cisco Crosswork UI.

License Authorization Statuses

Based on the registration status of your Crosswork Network Controller application, you can see the following License Authorization Statuses.

Table 24: License Authorization Statuses

Registration Status	License Authorization Status	Description
Unregistered	Evaluation mode	A 90-day evaluation period during which the licensed features of the application can be freely used. This state is initiated when you use the application for the first time.
	Evaluation Expired	The application has not been successfully registered at the end of the evaluation period. During this state, the application features are disabled, and you must register to continue using the application.
	Registered Expired	The application is unable to contact the CSSM before the expiration of Identity Certificates and has returned to the unregistered state. The application resumes the remaining evaluation period, if available. At this stage, new registration ID token is required to reregister the application.
Registered	Authorized (In Compliance)	The application has been fully authorized to use the reserved licensed features. The authorization is automatically renewed every 30 days.
	Out of Compliance	The associated Virtual Account does not have enough licenses to reserve for the application's current feature use. You must renew the entitlement/usage limit registered with the token to continue using the application.
	Authorization Expired	The application is unable to communicate with the CSSM for 90 days or more, and the authorization has expired.

Authorization Status Response

This section explains the actions or message enforced by Crosswork in case of "Out of Compliance" or "Evaluation Expired" status.

The behavior is covered for Right-to-Use (RTU) and Right-to-Manage (RTM) licenses.

Table 25: Out of compliance status action for registered systems

Registration Status	License Authorization Status	Solution or Product	Enforced Action or Message
Registered	Out of Compliance	Crosswork Network Controller (solution)	No action taken.
		Crosswork Optimization Engine	No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Active Topology	No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Service Health	No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Change Automation	RTU: No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork Health Insights	RTU: No action taken. A message is logged with license state indicating that "License usage has exceeded the limit".
		Crosswork External Collection	No action taken.
		Element Management Functions	RTM: No action taken (in case of normal token-based registration).

Table 26: Evaluation expired status action for unregistered systems

Registration Status	License Authorization Status	Solution or Product	Enforced Action or Message
Unregistered	Evaluation Expired	Crosswork Network Controller (solution)	All UI screens are disabled, and only the Smart Licensing window is displayed. Users can continue to use Crosswork Network Controller only after completing the registration.
		Crosswork Optimization Engine	Only READ operations are allowed. Create, update, and delete operations are restricted.
		Crosswork Active Topology	No action taken. No impact on provisioning UI (NSO) workflows.
		Crosswork Service Health	Monitoring cannot be enabled or resumed. An error message ("License evaluation expired or reservation exceeded, Service Health functionality disabled") is displayed.
		Crosswork Change Automation	RTU: Playbook execution is not allowed. A major alarm is raised.
		Crosswork Health Insights	RTU: Health Insights usage is not allowed. A message is logged with license state indicating that "License is expired". RTM: Critical alarm is raised.
		Crosswork External Collection	RTM: Collection Job creation, Template Collection Job creation, and Bulk template collection operation requests are rejected.
		Element Management Functions	RTM: ZTP API operations are not allowed. An error message is displayed ("Your License Evaluation Period has expired or there are no Reserved Licenses").

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 315).

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 388.

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 rule list for the device level NACM control will integrate Crosswork Network Controller with the NSO workflow. Note that for every unique combination of Device Access Group that is 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. You can also change the Cisco Crosswork administrator password using the following methods:

- Log in as the admin user and edit the admin user password .
- Enter the following command: `admin(config)# username admin <password>`

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 27: 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

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 316).

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 312). Later, you can edit the roles themselves to give users the privileges you want (see Edit User Roles, on page 316).

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

Step 2 Click on 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.

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.

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 28: Global API Permission Categories

Category	Global API Permissions	Description
AAA	Password Change APIs	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 APIs	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 APIs	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, and the DELETE permission allows you to delete a user or role.
Alarms **Attention** The Alarm APIs are deprecated in the Crosswork 6.0 release.	Alarms APIs	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 or acknowledged, 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.

Category	Global API Permissions	Description
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
Crosswork Network Controller	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, while 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 APIs	Primarily used to investigate issues in the overlay. Only READ permission is applicable.
	CAT UI APIs	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, while 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, while 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.), while 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.
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 add/update/delete the data.

Category	Global API Permissions	Description
Crosswork Optimization Engine	OPTIMA Analytics API	Allows you to manage analytics in Crosswork Optimization Engine. The READ permission allows you to view/export historical data, while WRITE permission enables you to change the Traffic Engineering Dashboard settings.
	Optimization Engine UI APIs	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.

Category	Global API Permissions	Description
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
Health Insights	Health Insights APIs	Allows you to manage Heath 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.
ICON Server	ICON Server APIs	Allows you to update the collection setting for interface/IP data collection intended for topology and optimization use cases.

Category	Global API Permissions	Description
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. 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 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.
	Distributed Cache APIs	The READ permission allows you to fetch cache statistics for troubleshooting.
	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 APIs	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 APIs	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.
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.
SWIM	SWIM NB API	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. • Get Service-Metric data 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.
	Heuristic Package Manager APIs	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.)

Category	Global API Permissions	Description
Zero Touch Provisioning	CW Config Service APIs	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.
	CW Image Service APIs	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
	CW ZTP Service APIs	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
CW-CLMS	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.

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.

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 388.

Manage WebSocket Subscriptions

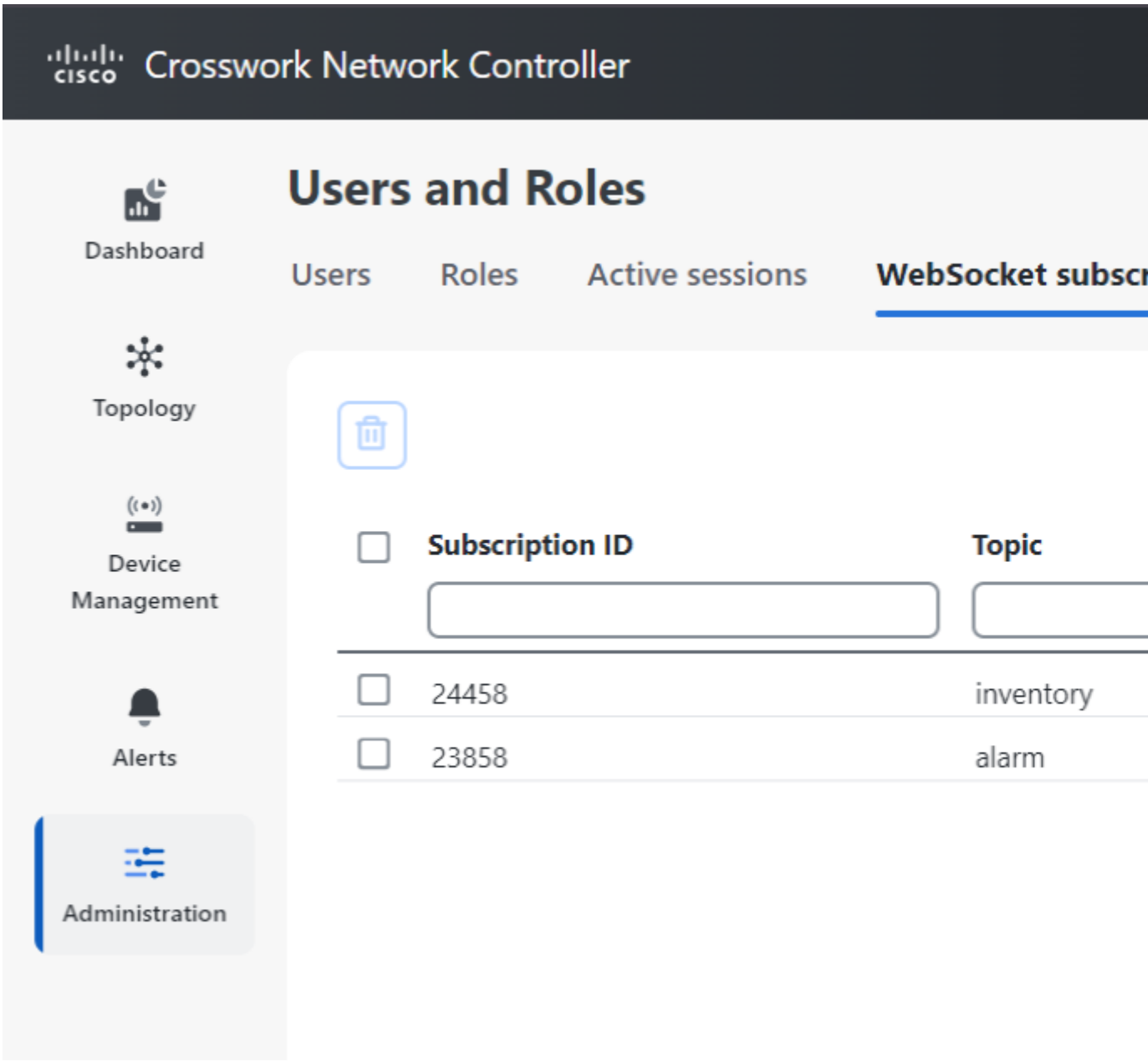
If you have subscribed to WebSocket subscriptions using **Basic Authentication** or **JWT** based authentication to authenticate and establish your connections, you can view these subscriptions in the Crosswork UI. The types of subscriptions that are supported are-

- Inventory
- Alarm
- Service Notification

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

Step 2 Click the **WebSocket subscriptions** tab.

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.

You can also choose to delete a subscription by using the **Delete** icon on this page.

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

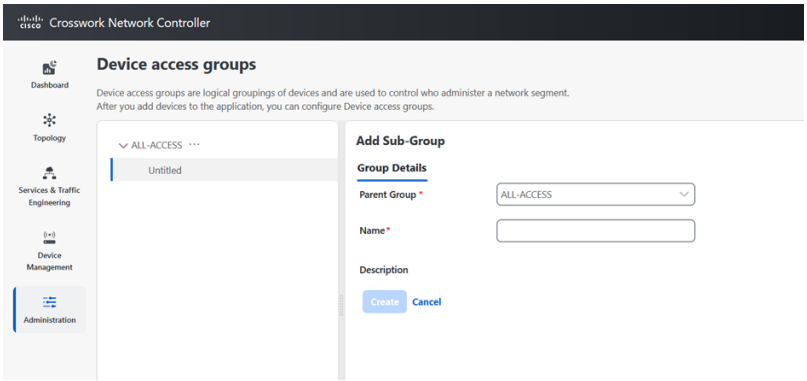
with NSO and Device Access Groups to streamline device configurations, using JWT tokens for authentication and authorization in RESTCONF and JSON-RPC API workflows. However, reverse synchronization is not possible; changes in NSO are not reflected in Crosswork Device Access Groups (for detailed information on the prerquisites for setting up NSO, see Configure NSO Servers, on page 335). External LDAP, TACACS, and RADIUS servers support Device Access Groups integration. For server configuration details, refer to the specific field description tables for each server in Set Up User Authentication (TACACS+, LDAP, and RADIUS), on page 343.

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.

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.

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.

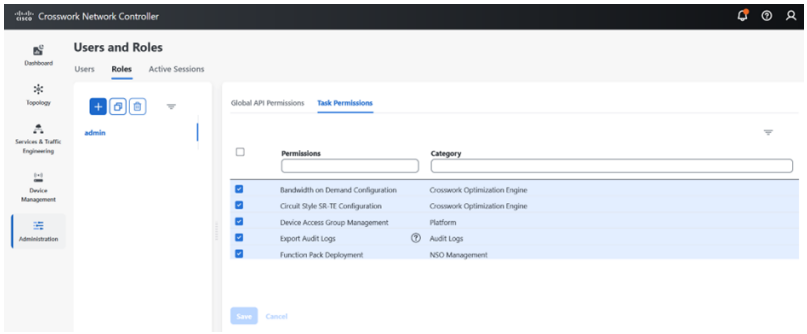
Assign Task permissions

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.

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 115: 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.

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 314 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 312 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 336
• Configure LSA NSO, on page 341

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.

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.

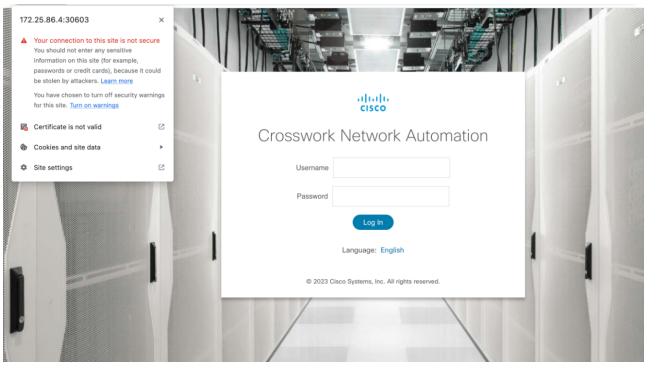
```
 <aaa>
    <package-authentication>
     <enabled>true</enabled>
     <packages>
       <package>cisco-cfp-jwt-auth</package>
     </packages>
    </package-authentication>
</aaa>
- Make sure to restart ncs for the configuration in ncs.conf to take effect:
   /etc/init.d/ncs restart
```

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 116: View Certificate Window



3. In the **Certificate Viewer** window, go to the **Details** tab.

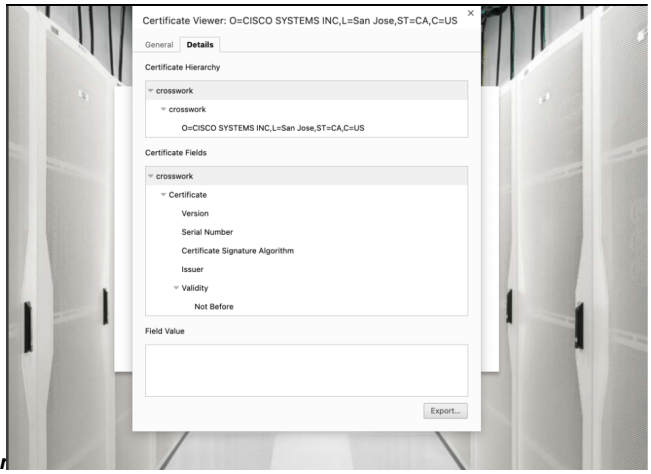
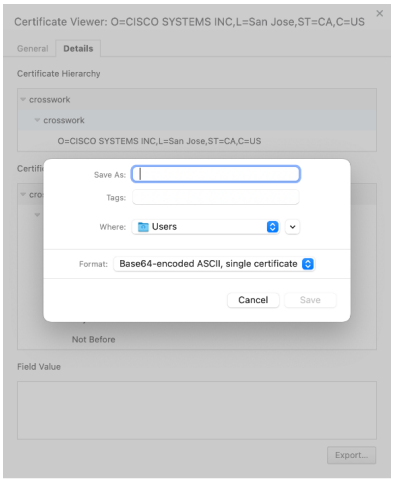


Figure 117: Details for Certificate Viewer

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 extension **.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 118: 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.

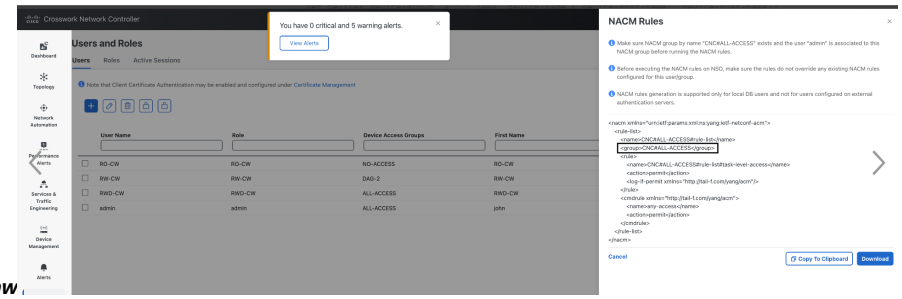
   Note that the ALL-ACCESS Device Access Group is not created by default, and is not needed for an admin user. If you want, you can create it manually using the following command, where **group-name** is the name of the group you create.

   ```
   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 119: 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.

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 336.

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.

Set Up User Authentication (TACACS+, LDAP, and RADIUS)

In addition to supporting local users, Crosswork Network Controller supports TACACS+, LDAP, and RADIUS users through integration with the TACACS+, LDAP, and RADIUS servers. The integration process has the following steps:

- Configure the TACACS+, LDAP, and RADIUS servers.
- Create the roles that are referenced by the TACACS+, LDAP, and RADIUS users.
- Configure AAA settings.
- You can also enable Single Sign-on (SSO) for authentication of TACACS+, LDAP, and RADIUS users. For more information, see Enable Single Sign-on (SSO), on page 356.
- You can create and manage Device Access Groups for users on these servers. For more information, see Manage Device Access Groups, on page 332.

Note

- The AAA server page works in bulk update mode wherein all the servers are updated in a single request. It is advised to give write permission for "Remote Authentication Servers Integration api" only to users who have the relevant authorization to delete the servers.
- A user with only Read and Write permissions (without 'Delete' permission) can delete the AAA server details from Cisco Crosswork since delete operations are part of 'Write' permissions. For more information, see Create User Roles, on page 315.
- While making changes to AAA servers (create/edit/delete), you are recommended to wait for few minutes between each change. Frequent AAA changes without adequate intervals can result in external login failures.
- Cisco Crosswork supports the configuration of up to 5 external servers.

Caution Please note that any operation you do following the instructions in this section will affect all new logins to the Crosswork user interface. To minimize session interruption, Cisco recommends that you perform all your external server authentication changes and submit them in a single session.

Manage TACACS+ Servers

Crosswork supports the use of TACACS+ servers to authenticate users.

You can integrate Crosswork with a standalone server (open TACACS+) or with an application such as Cisco ISE (Identity Service Engine) to authenticate using the TACACS+ protocols.

Before you begin

- Create Device Access Group to manage access to the AAA operations. For more information, see Create Device Access Groups, on page 333
- Configure the relevant parameters (user role, device access group attribute, shared secret format, shared secret value) in the TACACS+ server (standalone or Cisco ISE), before configuring the AAA server in Crosswork Network Controller. For more information on Cisco ISE procedures, see the latest version of Cisco Identity Services Engine Administrator Guide.

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **TACACS+** tab. From this window, you can add, edit, and delete a new TACACS+ server.

Step 2 **To add a new TACACS+ server**:

a) Click the + icon.

b) Enter the required TACACS+ server information.

Table 29: 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 value of the service that you are attempting to gain access to. For example, "raccess". This field is verified only for standalone TACACS+. In case of Cisco ISE, you can enter a junk value. Do not leave the field blank.

Field	Description
Policy Id	Enter the user role that you created in the TACACS+ server. **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	Device access group attribute value is based on the key used for device access group in (ISE/Standalone) TACACS+ server attributes. These values can be one or more than one comma separated values.
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).

See the example at the end of this topic for more details.

c) After you enter all the relevant details, click **Add**.
d) Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Step 3 **To edit a TACACS+ server**:

a) Click the checkbox next to the TACACS+ server and click  .
b) After making changes, click **Update**.

Step 4 **To delete a TACACS+ server**:

a) Click the checkbox next to the TACACS+ server and click  . The Delete *server-IP-address* dialog box opens.
b) Click **Delete** to confirm.

Example

In this example, the TACACS+ parameters are configured in Cisco ISE. As a prerequisite, a Device Access Group has been created in Crosswork to manage the AAA operation access.

The relevant TACACS+ parameters are configured in Cisco ISE:

- User profile: `role0` (to be used in *Policy Id* field)

- Device Access Group Attribute: `DAG-CONFIGURE`
- Shared secret format: `ASCII`

Figure 120: Configure TACACS+ Profile Attributes in Cisco ISE

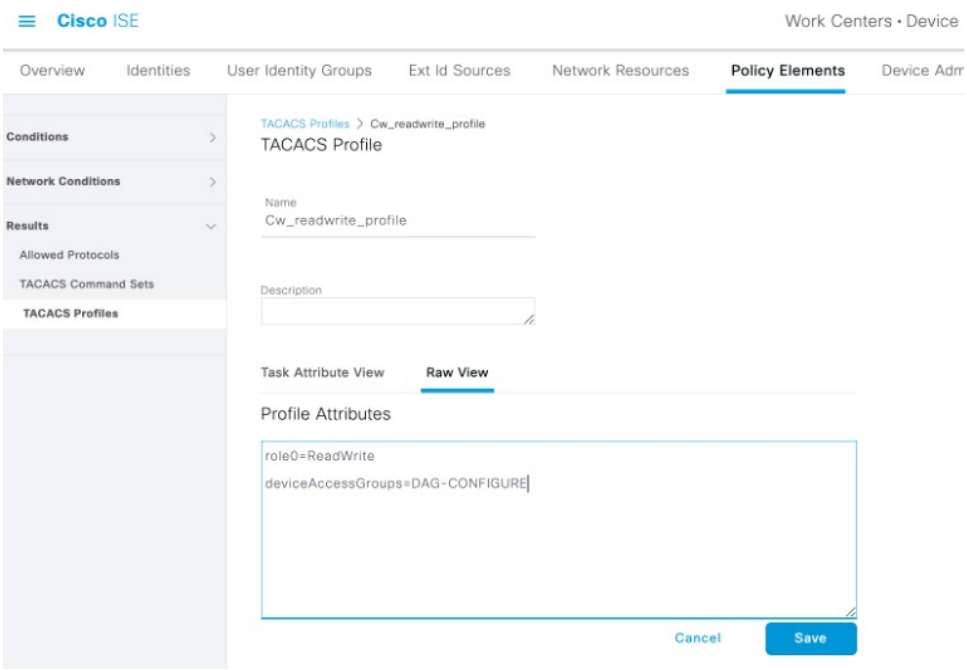
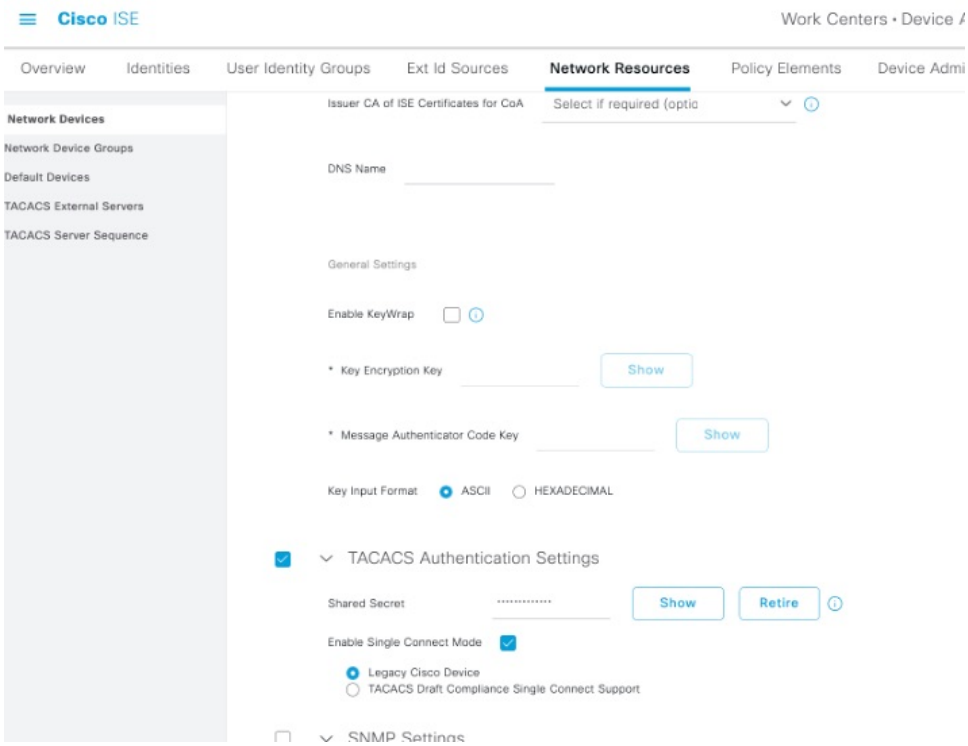
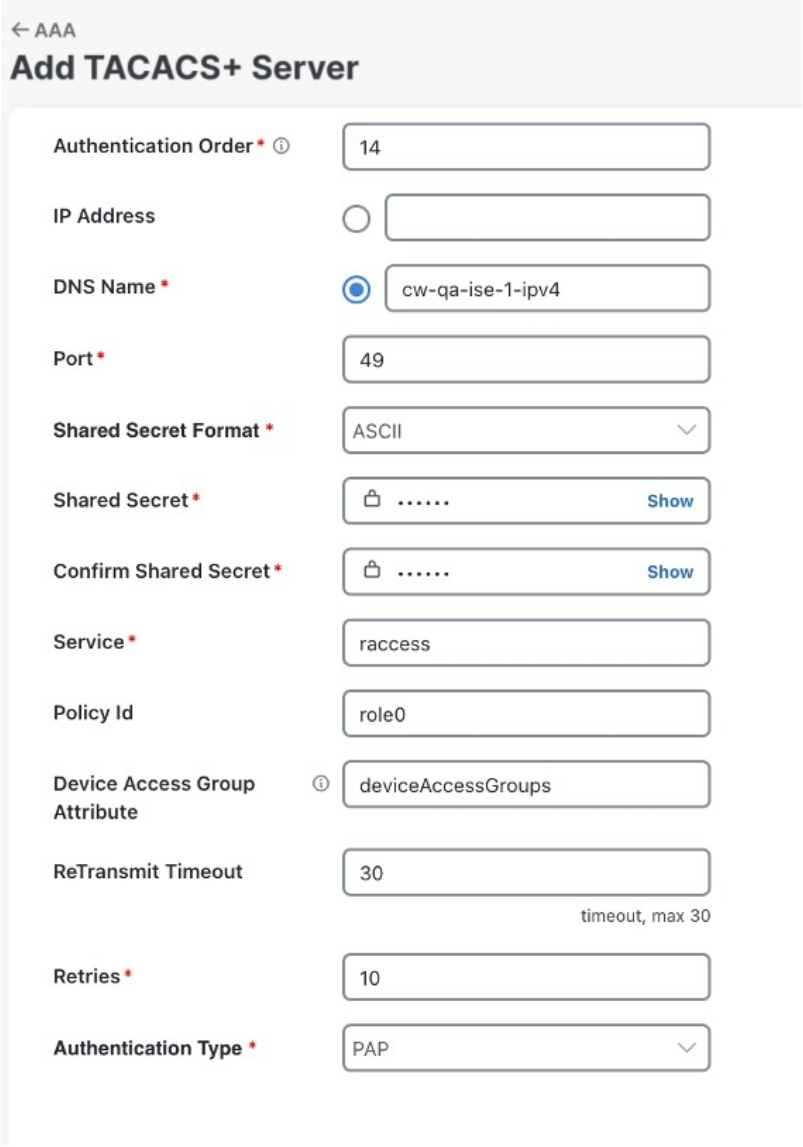


Figure 121: Configure TACACS+ Authentication Settings in Cisco ISE



Now, the TACACS+ server is added in Crosswork UI:

Figure 122: Add TACACS+ Server



Here is the sample API payload for the above 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",
            }
        ]
    }
}
```

```
-------------------------------------------------------------------------------------------------------------
CROSSWORK                                                 CISCO ISE
VALUE
-------------------------------------------------------------------------------------------------------------
Device Access Group Attribute=deviceAccessGroups    deviceAccessGroups=DAG-CONFIGURE
DAG-CONFIGURE
PolicyId=role0                                            role0=ReadWrite
ReadWrite
```

Manage LDAP Servers

Lightweight Directory Access Protocol (LDAP) is a server protocol used to access and manage directory information. Crosswork supports the use of LDAP servers (OpenLDAP, Active Directory, and secure LDAP) to authenticate users. It manages directories over IP networks and runs directly over TCP/IP using simple string formats for data transfer.

To use secure LDAP protocol, you must add **Secure LDAP Communication** certificate before adding the LDAP server. For more details on adding certificates, see Add a New Certificate, on page 295.

Before you begin

- Create Device Access Group to manage access to the AAA operations. For more information, see Create Device Access Groups, on page 333
- Configure the relevant parameters (bind DN, policy baseDN, policy id, device access group attribute, etc.) in the LDAP server before configuring the AAA server in Crosswork Network Controller.

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **LDAP** tab. Using this window, you can add, edit, and delete a new LDAP server.

Step 2 **To add a new LDAP server**:

a) Click the + icon.

b) Enter the required LDAP server details.

Table 30: LDAP 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.
Name	Name of the LDAP handler.
IP Address/ Host Name	LDAP server IP address or host name

Field	Description
Secure Connection	Enable the **Secure Connection** toggle button if you want to connect to the LDAP server via the SSL communication. When enabled, select the secure LDAP certificate from the **Certificate** drop-down list. **Note** The secure LDAP certificate must be added in the Certificate Management screen prior to configuring the secure LDAP server. This field is disabled by default.
Port	The default LDAP port number is 389. If Secure Connection SSL is enabled, the default LDAP port number is 636.
Bind DN	Enter the login access details to the database. Bind DN allows user to login to the LDAP server.
Bind Credential / Confirm Bind Credential	Username and password to login to the LDAP server.
Base DN	Base DN is the starting point used by the LDAP server to search for user authentication within your directory.
User Filter	The filter for user search.
DN Format	The format used to identify the user in base DN.
Principal Attribute ID	This value represents the UID attribute in the LDAP server user profile under which a particular username is organized.
Policy BaseDn	This value represents the role mapping for user roles within your directory.
Policy Map Attribute	This helps in identifying the user under the policy base DN. This value maps to the `userFilter` parameter in your LDAP server attributes.
Policy ID	The **Policy ID** field corresponds to the user role that you created in the LDAP server. **Note** If you try to login to Crosswork Network Controller as a LDAP user before creating the required user role, you will get the error message: "`Login failed, policy not found. Please contact the Network Administrator for assistance.`". To avoid this error, ensure to create the relevant user roles in the LDAP server, before setting up a new LDAP server in Crosswork.
Device Access Group Attribute	Device access group attribute value is based on the key used for device access group in LDAP server attributes. These values can be one or more than one comma separated values.
Connection Timeout	Enter the timeout value. Maximum timeout is 30 seconds.

See the example at the end of this topic for more details.

c) Click **Add**.

d) Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Step 3 **To edit a LDAP server**:

a) Select the LDAP server and click .
b) After making changes, click **Update**.

Step 4 **To delete a LDAP server**:

a) Select the LDAP server and click .
b) Click **Delete** to confirm.

Example

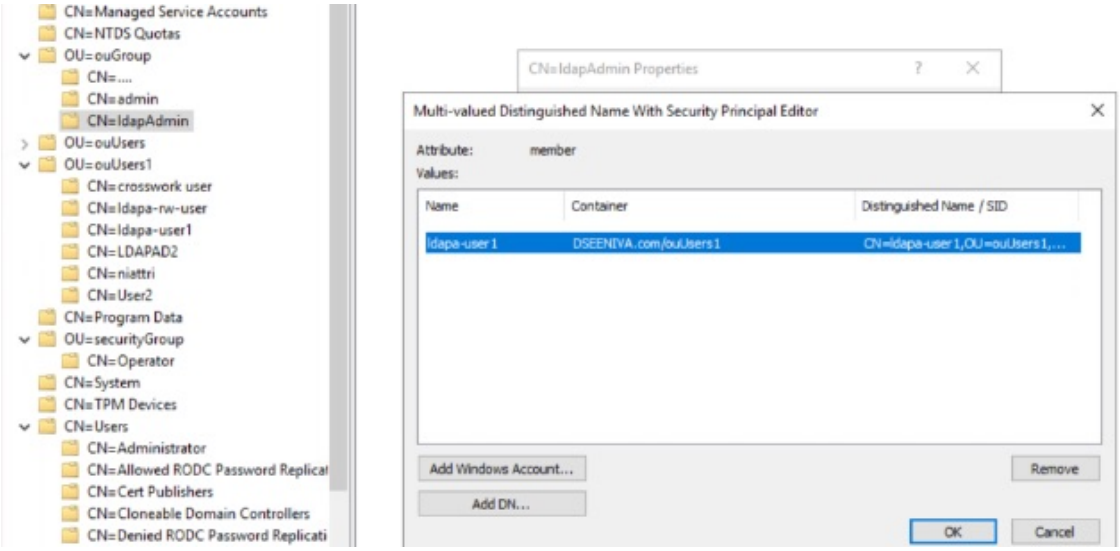
The below example shows the parameters entered for secure LDAP configuration. As a prerequisite, a Device Access Group has been created and configured in Crosswork to manage the AAA operation access.

The relevant parameters are configured in the LDAP server. Here are some of the key points:

- The user role is `ldapa-user1` and it belongs to the user group `ldapAdmin`.
- The username is this example is `DSEENIVA`.
- The policy id is `sAMAccountName`.
- The `ldapUrl` parameter is a combination of address and port
- The parameters under the `ldap_attr_server` section are used for role mapping. The `baseDN` parameter maps to the *Policy baseDN* field and the `userFilter` parameter maps to the *Policy Map Attribute* field in the Crosswork UI.
- The device access group is configured in LDAP server as `'Description='ALL-ACCESS'.`

The user group and user role mapping configured in LDAP server:

Figure 123: Add LDAP Server



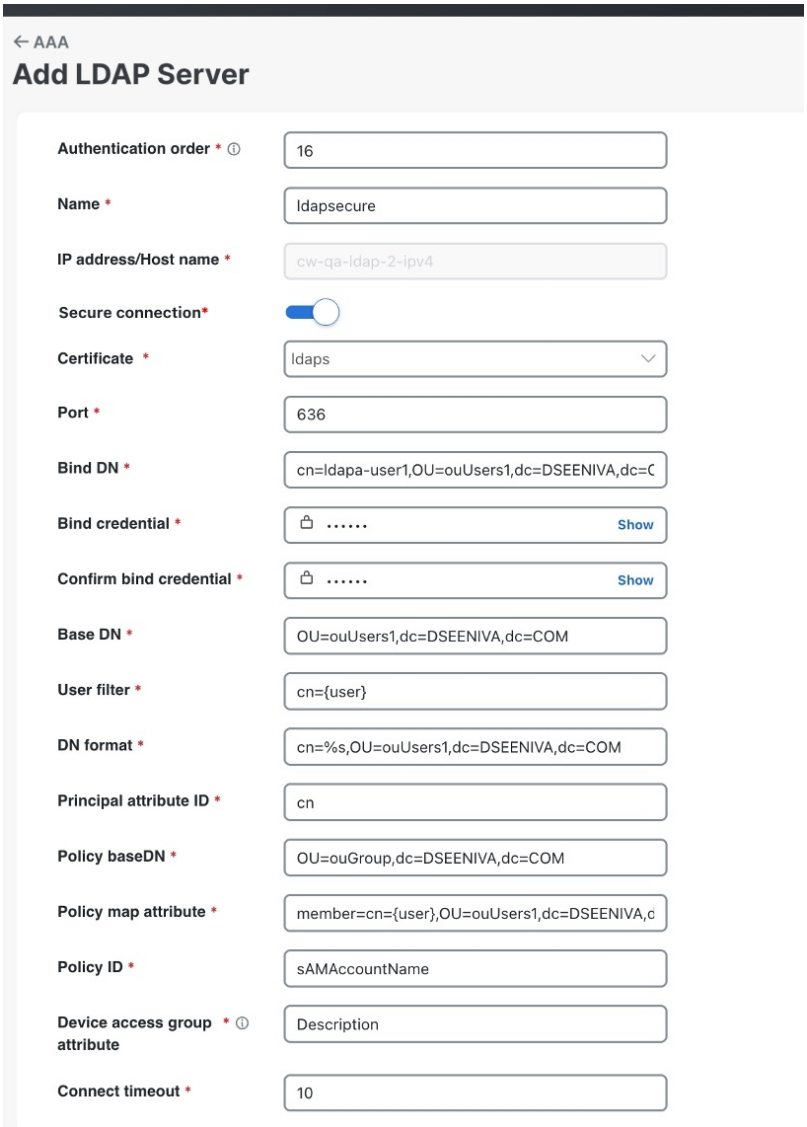
Here is the sample API payload for this example:

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

Here is the corresponding LDAP configuration in the Crosswork UI:

Figure 124: Add LDAP Server



Manage RADIUS Servers

Crosswork supports the use of RADIUS (Remote Authentication Dial-In User Service) servers to authenticate users. You can also integrate Crosswork with an application such as Cisco ISE (Identity Service Engine) to authenticate using the RADIUS protocols.

Before you begin

- Create Device Access Group to manage access to the AAA operations. For more information, see Create Device Access Groups, on page 333
- Similar to TACACS+ server, you must configure the relevant parameters (user role, device access group attribute, shared secret format, shared secret value) in the RADIUS server before configuring the AAA server in Crosswork Network Controller. For more information on Cisco ISE procedures, see the latest version of Cisco Identity Services Engine Administrator Guide.

Step 1 From the main menu, select **Administration** > **AAA** > **Servers** > **RADIUS** tab. From this window, you can add, edit, and delete a new RADIUS server.

Step 2 **To add a new RADIUS server**:

a) Click the  icon.

b) Enter the required RADIUS server information.

Table 31: 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 TACACS+ 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.
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 value of the service that you are attempting to gain access to. For example, "`raccess`".

Field	Description
Policy Id	The **Policy Id** field corresponds to the user role that you created in the RADIUS server. **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	Device access group attribute value is based on the key used for device access group in RADIUS server attributes. These values can be one or more than one comma separated values.
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 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).

As RADIUS configuration is very similar to TACACS+, please refer to the detailed example in the Manage TACACS+ Servers, on page 343 for more information.

c) After you enter all the relevant details, click **Add**.
d) Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

Step 3 **To edit a RADIUS server**:

a) Click the checkbox next to the RADIUS server and click  .
b) After making changes, click **Update**.

Step 4 **To delete a RADIUS server**:

a) Click the checkbox next to the RADIUS server and click  . The Delete *server-IP-address* dialog box opens.
b) Click **Delete** to confirm.

Configure AAA Settings

Users with relevant AAA permissions can configure the AAA settings.

Step 1 From the main menu, choose **Administration** > **AAA** > **Settings** .

Step 2 Select the relevant setting for **Fallback to Local**. By default, Crosswork prefers external authentication servers over local database authentication.

Note Admin users are always authenticated locally.

Step 3 Select the relevant value for the **Logout All Idle Users After** field. Any user who remains idle beyond the specified limit will be automatically logged out.

Note The default timeout value is 30 minutes. If the timeout value is adjusted, the page will refresh to apply the change.

Step 4 Enter a relevant value for the **Number of Parallel Sessions**.

Note Crosswork 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.

Note Crosswork supports 50 simultaneous NBI sessions up to 400 sessions (in Crosswork Network Controller version 4.1.x) and 500 sessions (in Crosswork Network Controller version 5.0.x).

Step 5 Check the **Enable source IP for auditing** check box to log the IP address of the user (source IP) for auditing and accounting. This check box is disabled by default. Once you enable this option and relogin to Cisco Crosswork, you will see the **Source IP** column on 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 , and the lockout duration. Users can attempt to login with the correct credentials once the wait time is over.

Enable Single Sign-on (SSO)

Single Sign-on (SSO) is an authentication method that allows you to log in with a single ID and password to any of several related, yet independent, software systems. It allows you to log in once and access the services without reentering authentication factors. Cisco Crosswork acts as Identity Provider (IDP) and provides authentication support for the relying service providers. You can also enable SSO for authentication of TACACS+, LDAP, and RADIUS users.

Crosswork supports SSO cross-launch to enable easier navigation with the service provider. Once configured, the URL can be launched using the launch icon ( ) located at the top right corner of the window.

Attention

- When Crosswork is re-installed, you must ensure that the latest IDP metadata from Crosswork is updated to the service provider applications. Failing to do this will result in authentication failure due to mismatched metadata information.
- First-time login users cannot switch to using a different username before mandatorily changing the password. The only workaround is for the administrator to terminate the session.

When Crosswork is re-installed, you must ensure that the latest IDP metadata from Crosswork is updated to the service provider applications. Failing to do this will result in authentication failure due to mismatched metadata information.

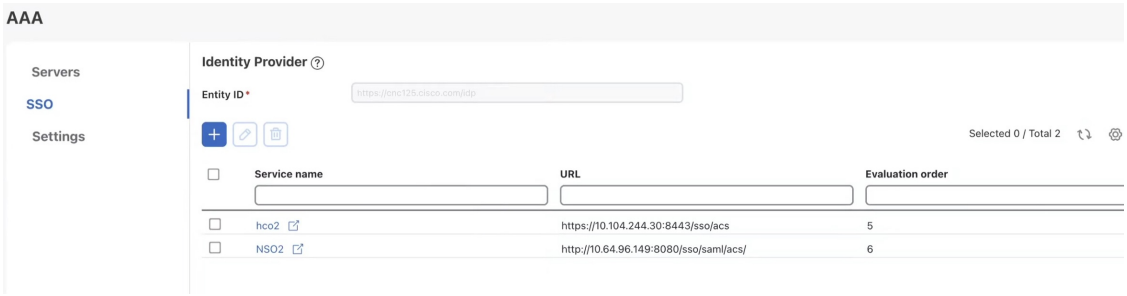
Note The Cisco Crosswork login page is not rendered when the Central Authentication Service (CAS) pod is restarting or not running.

Before you begin

Ensure that the **Enable source IP for auditing** check box is selected on the **Administration** > **AAA** > **Settings** page.

Step 1 From the main menu, choose **Administration** > **AAA** > **SSO**. The **Identity Provider** window is displayed. Using this window, you can add, edit settings, and delete service providers.

Figure 125: 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**: Enter the name of the service provider entity.

  Note If a URL is provided, the **Service name** column entry in the **Identity Provider** window becomes a hyperlink.

- **Evaluation Order**: Enter a unique number which indicates the order in which the service definition should be considered.

- **Metadata**: Click the field, or click **Browse** to navigate to the metadata XML document that describes a SAML client deployment. You can also enter the service provider URL here for cross-launch.

Step 3 Click **Add** to finish adding the service provider.

Step 4 Click **Save All Changes**. You will be prompted with a warning message about restarting the server to update the changes. Click **Save Changes** to confirm.

After the settings are saved, when you log into the integrated service provider application for the first time, the application gets redirected to the Cisco Crosswork 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 5 **To edit a service provider:**

a) Click the check box next to the service provider and click . You can update the Evaluation Order and Metadata values as required.
b) After making changes, click **Update**.

Step 6 **To delete a service provider**:

a) Click the check box next to the service provider and click .
b) Click **Delete** to confirm.

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:

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 7.0 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. For more information, see Add a New Certificate, on page 295.

Step 1 From the main menu, choose a **Administration** > **Settings** > **System Settings** tab.

Step 2 Under **Server**, click the **Syslog Configuration** option.

Step 3 Click +.

Step 4 Enter Syslog configuration details. For more information, click ⓘ next to each option.

Use the **Criteria** option to define the scope and range of which kind of events should be forwarded as a syslog. For example: **(EventSeverity<2 or EventSeverity>=5) and OriginAppId=capp-infra and EventCategory=1**

The expression sends events as a syslog only if the event originates from the Infrastructure Platform, the category is the system, and the severity is either less than 2 or is equal or above 5.

Caution Expressions are freeform and not validated.

Step 5 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 32: 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 PID = 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 a traps, per consumer.
- Define the rate of which traps are forwarded to the consumer.

For more information on trap handling, see Enable Trap Handling, on page 386.

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:

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings** tab.

Step 2 Under **Server**, click the **Trap servers** option.

Step 3 Click  .

Step 4 Enter Trap server details. For more information, click  next to each option.

Use the **Criteria** option to define scope and range of which kind of events should be forwarded as a trap.

Click **Events and Alarms examples** for more information on the attributes used to raise an event.

Step 5 After entering all the relevant information, click **Add**.

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:

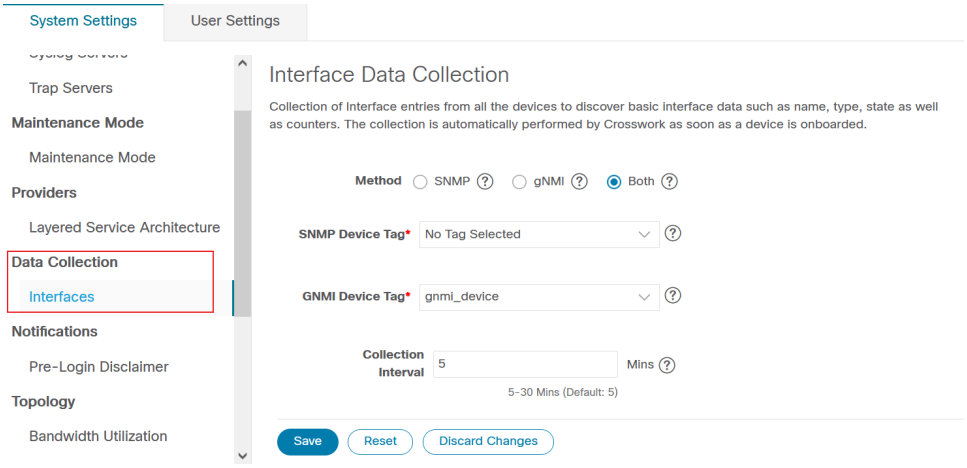
Before you begin

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, on page 270 and Apply or Remove Device Tags, on page 272.

Step 1 From the main menu, choose **Administration** > **Settings** > **System Settings** tab.

Step 2 Under **Data Collection**, select **Interfaces**.

Figure 126: Interface Data Collection Window



Step 3 In the **Interface Data Collection** 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 log in. The banner may remind 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.

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** checkbox.

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 will 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** checkbox.

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.

Note This feature is currently only supported for the EPNM application. For more information about the enabling scenarios, please refer to the EPNM user documentation.

Step 1 To enable FTP server:

a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **File Servers**

b) Under FTP, select on the **Enable** radio button.

c) Click **Save** to save your settings.

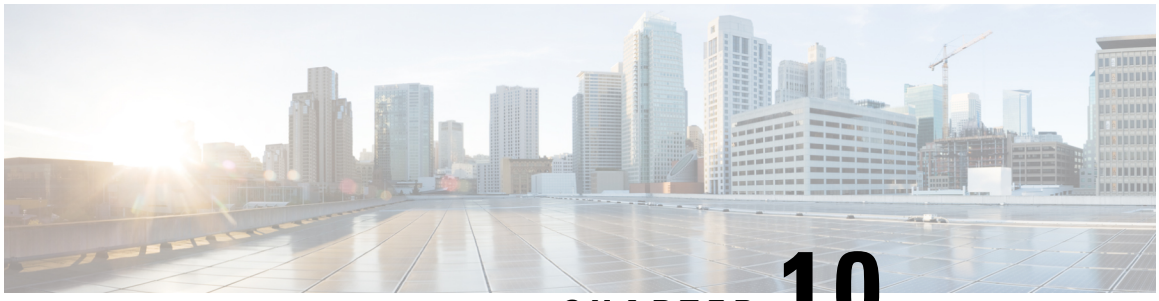
Step 2 To enable SFTP server:

a) From the main menu, choose **Administration** > **Settings** > **System Settings** > **File Servers**

b) Drag the **Enable Server Upload** slider to **On** position.

Caution SFTP supports upload option that allows write access to the Cisco Crosswork storage from the outside. You are recommended to 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 10

Manage System Health

This section contains the following topics:

Monitor System and Application Health

The Crosswork Platform is built on an architecture consisting of microservices. Due to the nature of these microservices, there are dependencies across various services within the Crosswork system. The system and applications are considered Healthy if all services are up and running. If one or more services are down, then the health is considered Degraded. If all services are down, then the health status is Down.

From the main menu, choose **Crosswork Manager** to access the **Crosswork Summary** and **Crosswork Health** windows. Each window provides various views to monitor system and application health. It also supplies tools and information that, with support and guidance from your Cisco Customer Experience account team, you can use 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

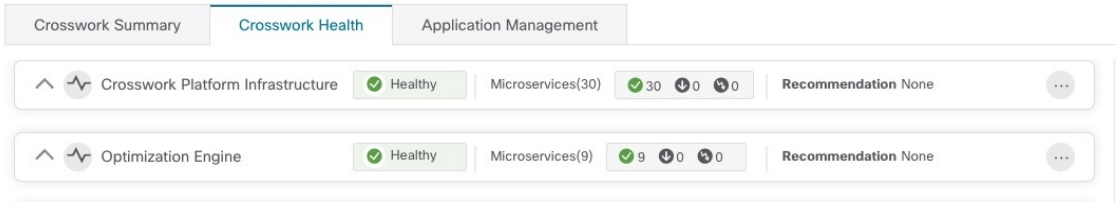
At a glance, the **Crosswork Summary** window (**Crosswork Manager** > **Crosswork Summary**) shows a summary of the overall system health. The main purpose of the **Crosswork Summary** window is to view Crosswork Cluster health in terms of hardware resources and VMs. For example, prior to installing or upgrading applications, you may want to check if the hardware resources are healthy and the VMs are running well. After clicking the **System Summary** tile, you can visually see resource utilization and drill down on VMs to perform some VM or cluster-related activities. In another case, you may see degrading services or over utilization of hardware resources. At this point, from a hardware point of view, you might find that the number of VMs in the system is insufficient prompting you to add more VMs to scale the system further out. For more information, see Cluster Management Overview, on page 23.

In addition to accessing Crosswork Cluster health, you can click on the **Cisco Crosswork Platform Infrastructure** and application tiles to view more details such as microservices and alarms.

Monitor Platform Infrastructure and Application Health

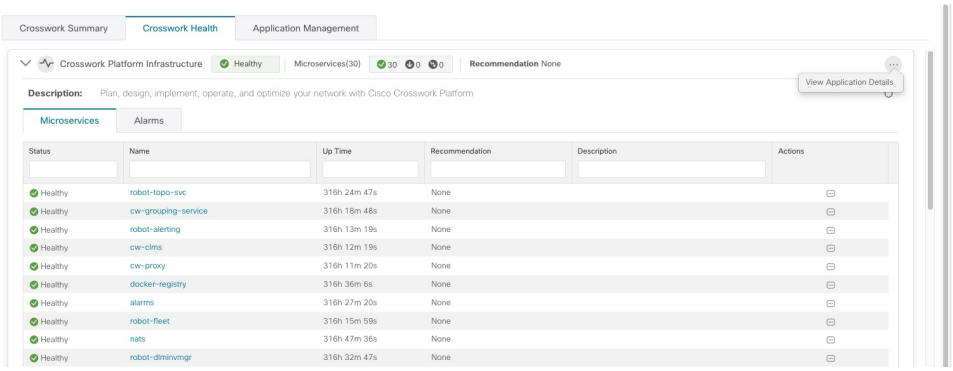
The **Crosswork Health** window (**Crosswork Manager** > **Crosswork Health** tab) provides health summaries for the Cisco Crosswork Platform Infrastructure and installed applications with the addition of microservice status details.

Figure 127: Crosswork Health tab



Within this window, expand an application row to view information on microservices, alarms, and events on that Crosswork product.

Figure 128: Microservices Tab



From the **Microservices** tab:

- 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 per microservice.

Note Showtech logs must be collected separately for each application.

From the **Alarms** tab:

- Filter the active alarms.
- Click the alarm description to drill down on alarm details.
- Change status of the alarms (Acknowledge, Unacknowledge, Clear)

- Add notes to alarms.
- View list of events in the product.
- View the coorelated 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. They give you a 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, categorized by the type of functionality they monitor and the metrics they provide. The following table lists some categories that may be available depending on whichCrosswork Network Controller applications are installed.

Table 33: 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.

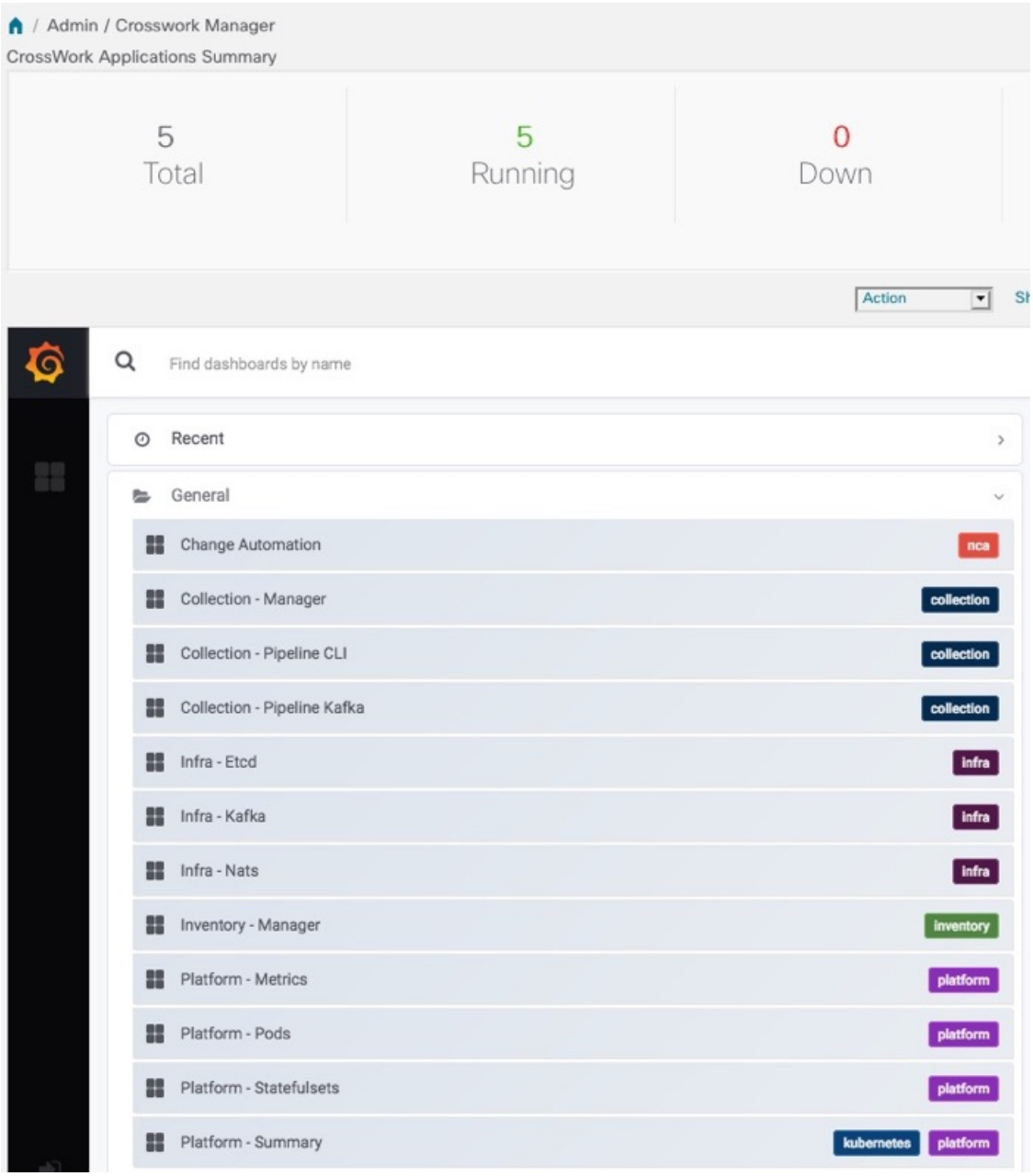
Grafana is an open-source visualization tool. The following provides general information about how to use the Crosswork Network Controller implementation of Grafana. For more information about Grafana itself, see https://grafana.com and http://docs.grafana.org

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

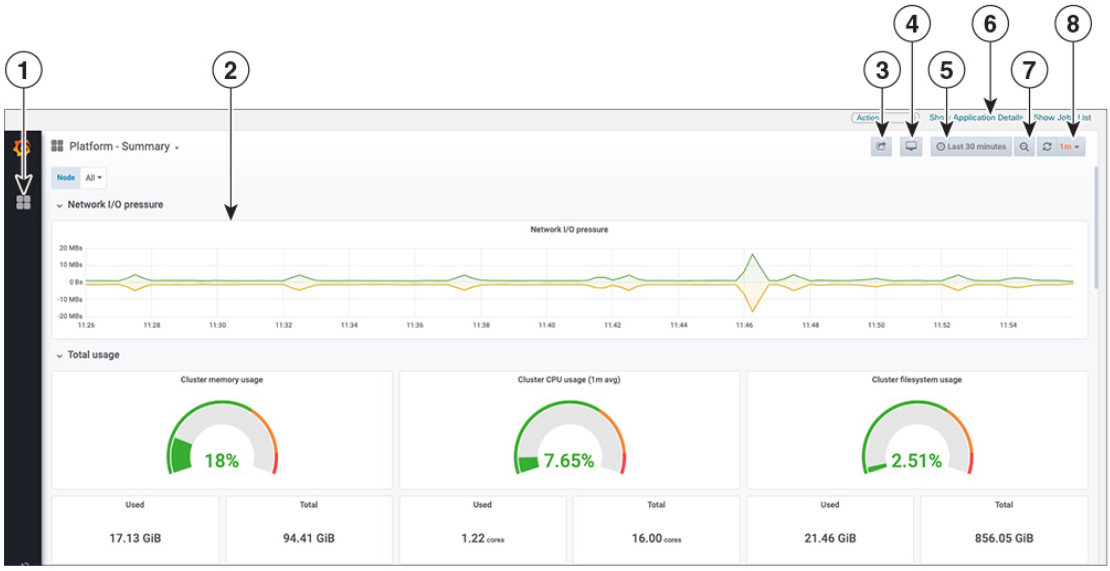
Step 2 At the top right, click **View more visualizations**.

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 the following example.



Step 4 Click the the dashboard you want to view. For example: Clicking on **Platform - Summary** dashboard displays a view like the one shown in the following figure.



Step 5 Scroll the dashboard as needed to display all of the metrics it provides, 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 will appear 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 popup 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**: Immediately or choose time interval to refresh the data shown. You can choose predefined refresh rates from **Off** to **2 Days**.

Check System Health Example

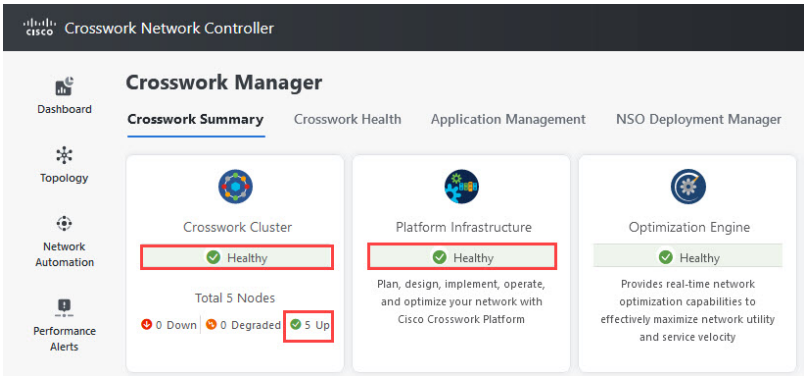
In this example, we navigate through the various windows and what areas should be checked for a healthy Crosswork system.

Step 1 Check overall system health.

a) From the main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary** tab.

b) Check that all the nodes are in Operational state (Up) and that the Crosswork Cluster and Platform Infrastructure is Healthy.

Figure 129: Crosswork Summary

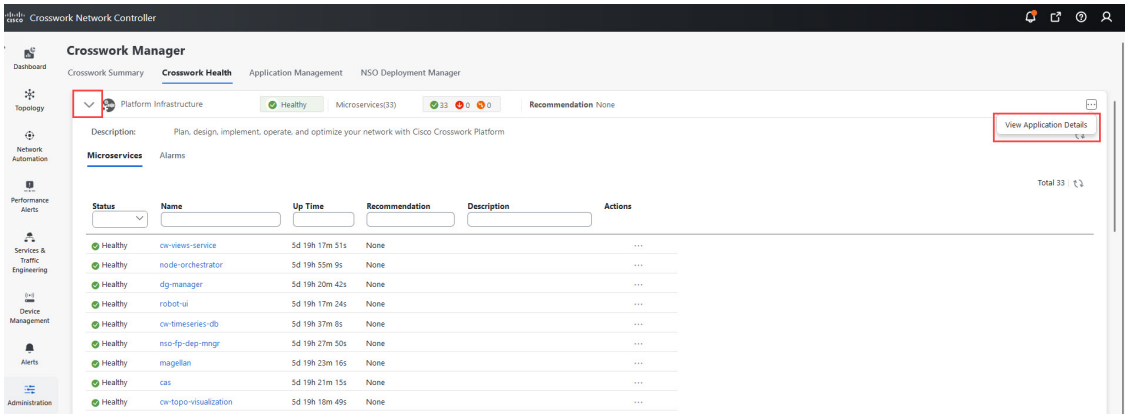


Step 2 Check and view detailed information about the microservices that are running as part of the Crosswork Platform Infrastructure.

a) Click the **Crosswork Health** tab.

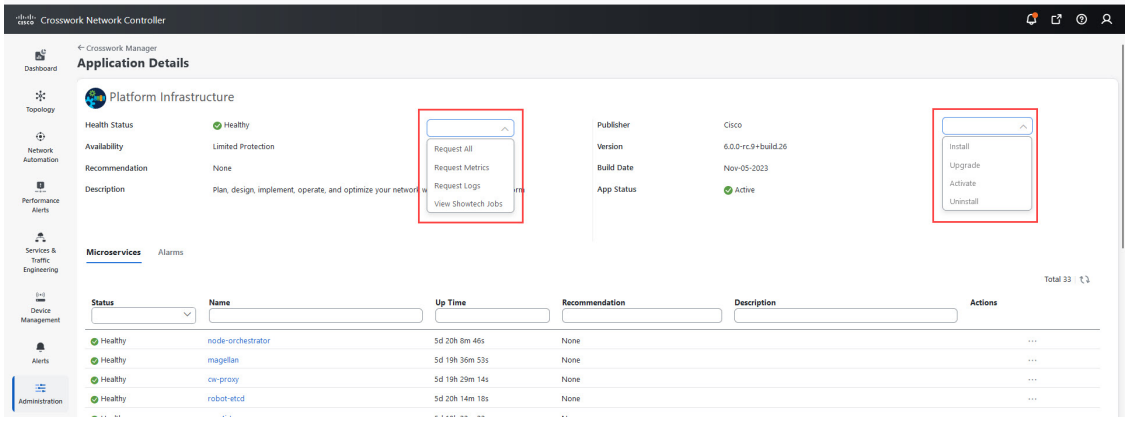
b) Expand the Crosswork Platform Infrastructure row, click ⋯, and select **Application Details**.

Figure 130: Crosswork Health



c) 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.

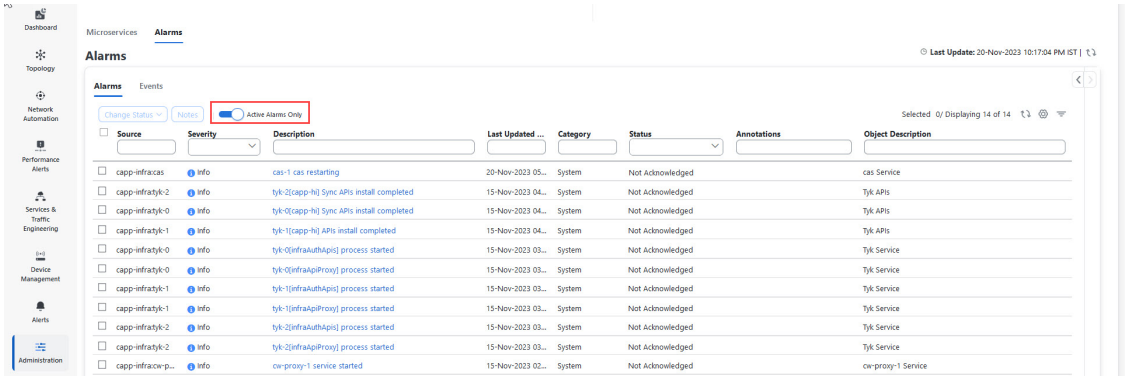
Figure 131: Application Details



Step 3 Check and view the alarms and events related to the microservices.

a) Click the **Alarms** tab. The list only displays Crosswork Platform Infrastructure alarms. You can further filter the list by viewing only active alarms.

Figure 132: Alarms



b) Click the **Events** tab. The list displays all Crosswork Platform Infrastructure events, and their coorelated alarms.

Step 4 View which Crosswork applications are installed.

a) 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 File (.tar.gz)** to install more applications.

Step 5 View the status of jobs.

a) 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.

View System Alarms

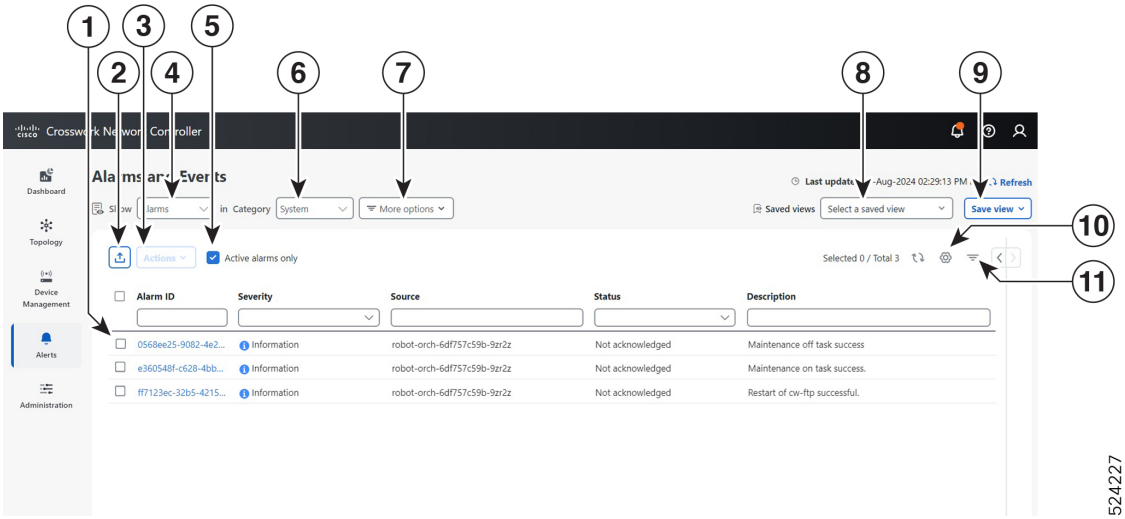
You can view the **Alarms and Events** window by navigating to one of the following:

- 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 7.0 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 in the figure below.

Figure 133: Alarms and Events window



Item	Description
1	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.
2	Click the icon to export a PDF or CSV file listing full information for all the alerts shown in the window. If you have one or more alerts selected at the time you click the icon, the file will contain information for the selected alerts only.
3	On the **Alarms** window only: Click the **Actions** dropdown 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	Toggles between the **Alarms** and **Events** windows.

Item	Description
5	On the **Alarms** window only: Select the **Active Alarms only** checkbox to display all active alarms.
6	Click on **Category** drop-down list to select the alarm category (**System**, **Network**, or **Devices**). The default selection is **System**.
7	Click on **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	Click in the **Saved Views** field to manage the previously saved views created using the **Save View** button. The popup **Manage Saved Views** window allows you to view, sort, see all views or only those you have saved.
9	Click the **Save View** button to save the current view. Crosswork will prompt you to enter and save the view under a unique name.
10	Click the ⚙ to select which columns to display in the alerts list.
11	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 has a Syslog feature that forwards system-related events to an external server (see Configure a Syslog Server, on page 362 and Configure a Trap Server, on page 363).

All the events related to the Crosswork platform are classified broadly into three categories: Day 0, Day 1, and Day 2. The following table lists the event categories (day 0, day 1, and day 2) and sample events or actions within that category:

Note See the Cisco Crosswork Network Controller Supported Alarms and Events document for the complete list of supported alarms and events.

Table 34: Event Classification

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
Day 2 – Events related to system operations and maintenance.	• Node eviction • Node eviction clean up fails • Deactivating an application fails • Uninstallation of an application fails • Slow disk or network • Node removal • Node insertion • Node drain fails • K8S ETCD clean up • Node removal fails • Node deletion fails • Deactivating an application successfully • Uninstalling an application successfully

Sample Day 0, Day 1, and Day 2 Events

The following 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 35: 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 36: 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

Table 37: 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 38: Adding an Application—Success

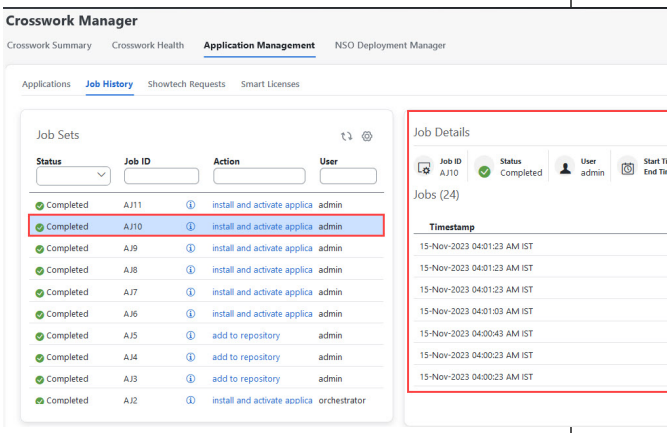
Severity	Information
Description	This event occurs when an application is added successfully.
Alarm	
Syslog Message	`<time_stamp> <hosting_hybrid_node> <time_stamp> <crosswork_VIP> CLUSTER-CLUSTER - 627b2140-a906-4a96-b59b-1af22f2af9f6 CLUSTER-99 'job_type=INSTALL_AND_ACTIVATE_APPLICATION,manager=app_manager:,user=admin,policyId=admin,backend=local,loginTime=2021-02-28T09:34:54Z,payload={"package_identifier":{"id":"cappztp","version":"1.1.0-prerelease.259+build.260"}} [accepted]'`
Recommendation	None

Table 39: Adding an Application—Failure

Severity	Information
Description	This event occurs when an application cannot be added.

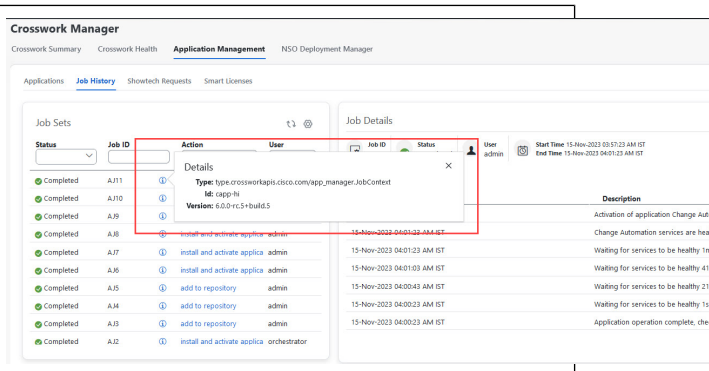
Sample Alarm	
Sample Syslog Message	None
Recommendation	After fixing the error, try adding the application again.

Table 40: 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 41: 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 42: 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 43: 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 44: 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 45: 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 46: 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 47: 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 48: 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 49: 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 50: 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 51: 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 52: 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 53: 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.

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 7.0 Device Lifecycle Management* guide.

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

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.

Enable Trap Handling

In addition to UI options, REST APIs, and Syslogs, Cisco Crosswork also provides the capability to generate SNMP traps for the events/alarms to notify the application and cluster health.

Crosswork supports using SNMPv3 and SNMPv2 to send the traps. The alarms and events are filtered based on the criteria set by user and converted to traps and sent to the trap server (see Configure a Trap Server, on page 363) using the alarm model in CISCO-EPM-NOTIFICATION-MIB. For more information, see Cisco EPM Notification MIB, on page 433.

Collect Audit Information

Audit logs map user information with all the critical user actions performed in the system. To view application Showtech logs, see Monitor Platform Infrastructure and Application Health, on page 368.

The audit log includes user actions related to the following 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)
- Cisco Crosswork Change Automation and Health Insights:
  - Manage playbooks (import, export, or delete) and playbook execution.

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, and configuration updates
  - Enabling and disabling of KPI Profiles
- Cisco Crosswork Optimization Engine:
  - SR-TE policy and RSVP TE tunnel creation, deletion, and configuration updates
  - Affinity mapping configuration

- Bandwidth on Demand and Bandwidth Optimization function and configuration updates
- RESTCONF API creation, deletion, and configuration updates

Sample Cisco Crosswork Change Automation and Health Insights Audit Log Entry

The following is a sample audit log entry created when a local admin user runs a playbook.

```
time="2020-06-09 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="2020-06-09T20:27:11Z" 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
```

Sample Cisco Crosswork Optimization Engine Audit Log Entries

Crosswork Optimization Engine UI Audit Log Entry Example

```
2020-06-12 02:48:07,990 INFO c.c.s.o.e.AuditLogger [http-nio-8080-exec-3] time=2020-06-12
02:48:07.000990 message=SR Policy created successfully. user=admin policyId=admin
backend=local loginTime=1591929794
{data={"headEnd":"192.168.0.2","endPoint":"192.168.0.6","color":"999","description":"","profileId":"","bindingSid":"333",
 "path":{"type":"dynamic","pathName":"Automation_validating_sr","metric":"IGP",
"affinity":[{"constraintType":"EXCLUDE_ANY","affinity":[31]}],"disjointness":{"disjointType":"",
 "associationGroup":"","subId":""}, "protectedSegment":"SEG_PROTECTED"}}}
```

Crosswork Optimization Engine RESTCONF API Audit Log Entry Example

```
time="2020-06-06 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
```

Table 54: 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 shorter and independent of time zones.

Field	Description
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 sample Crosswork Optimization Engine UI audit log is in the `optima-uiservice` 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 are once each hour. Crosswork stores them as separate gzipped tar files in the following 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

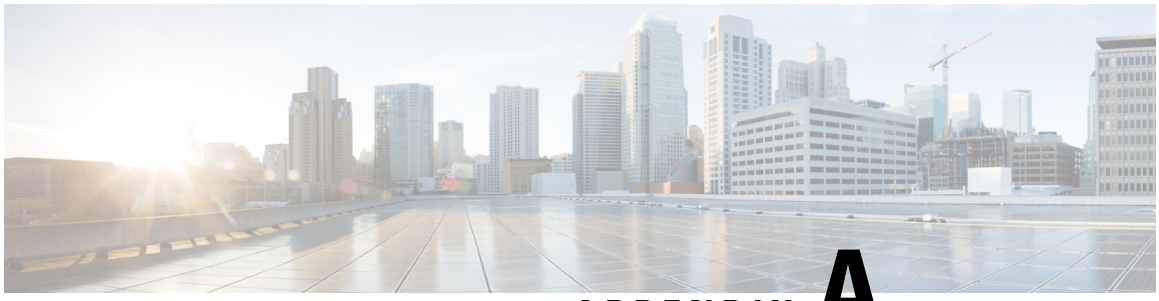
To view the audit log, perform the following steps:

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.



APPENDIX A

Configure Crosswork Data Gateway Instance

A Crosswork Data Gateway instance is created as a standalone instance and can be geographically separate from the controller application (the controller application could be Cisco Crosswork Infrastructure or Crosswork Cloud). This instance is capable of connecting to the controller application which will enable data collection from the network.

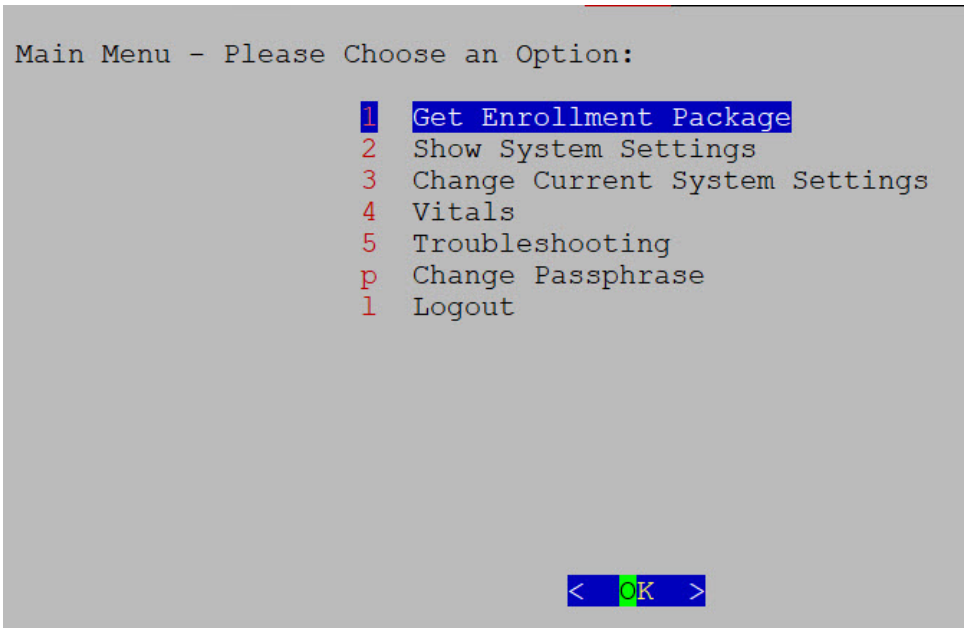
This chapter contains the following topics:

Use the Interactive Console

Cisco Crosswork Data Gateway launches an interactive console upon successful login. The interactive console displays the **Main Menu** as shown in the following figure:

Note The Main Menu shown here corresponds to **dg-admin** user. It is different for **dg-oper** user as the operator does not have same privileges as the administrator. See Table Table 55: Permissions Per Role, on page 393.

Figure 134: Interactive Console - Main Menu



The Main Menu presents the following options:

1. Get Enrollment Package

2. Show System Settings

3. Change Current System Settings

4. Vitals

5. Troubleshooting

p. Change Passphrase

l. Log out

Important When using an IPv6 address, it must be surrounded by square brackets ([1::1]).

Manage Crosswork Data Gateway Users

This section contains the following topics:

Supported User Roles

Crosswork Data Gateway supports only two users with the following user roles:

- **Administrator**: One default **dg-admin** user with administrator role is created when Crosswork Data Gateway is brought up for the first time. This user cannot be deleted and has both read and write privileges such as starting and shutting down the Crosswork Data Gateway VM, registering an application, applying authentication certificates, configuring server settings, and performing a kernel upgrade.
- **Operator**: The **dg-oper** user is also created by default during the initial VM bring up. This user can review the health of the Crosswork Data Gateway, retrieve error logs, receive error notifications and run connectivity tests between Crosswork Data Gateway instance and the output destination.

Note

- User credentials are configured for both the user accounts during Crosswork Data Gateway installation.
- Users are locally authenticated.

The following table shows the permissions available to each role:

Table 55: Permissions Per Role

Permissions	Administrator	Operator
Get Enrollment Package	✓	✓
Show system settings		
vNIC Addresses NTP DNS Proxy UUID Syslog Certificates First Boot Provisioning Log Timezone	✓	✓
Change Current System Settings		

Permissions	Administrator	Operator
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		
Docker Containers Docker Images Controller Reachability NTP Reachability Route Table ARP Table Network Connections Disk Space Usage Linux services NTP Status System Uptime	✓	✓
Troubleshooting		

Permissions	Administrator	Operator
Run Diagnostic Commands	✓	✓
Run show-tech	✓	✓
Remove All Non-Infra Containers and Reboot VM	✓	×
Reboot VM	✓	×
Export auditd logs	✓	✓
Re-enroll Data Gateway	✓	✓
Enable TAC Shell Access	✓	×
Change Passphrase	✓	✓

Change Passphrase

Both administrator and operator users can change their own passphrases but not each others'.

Follow these steps to change your passphrase:

Step 1 From the Main Menu, select **Change Passphrase** and click **OK**.

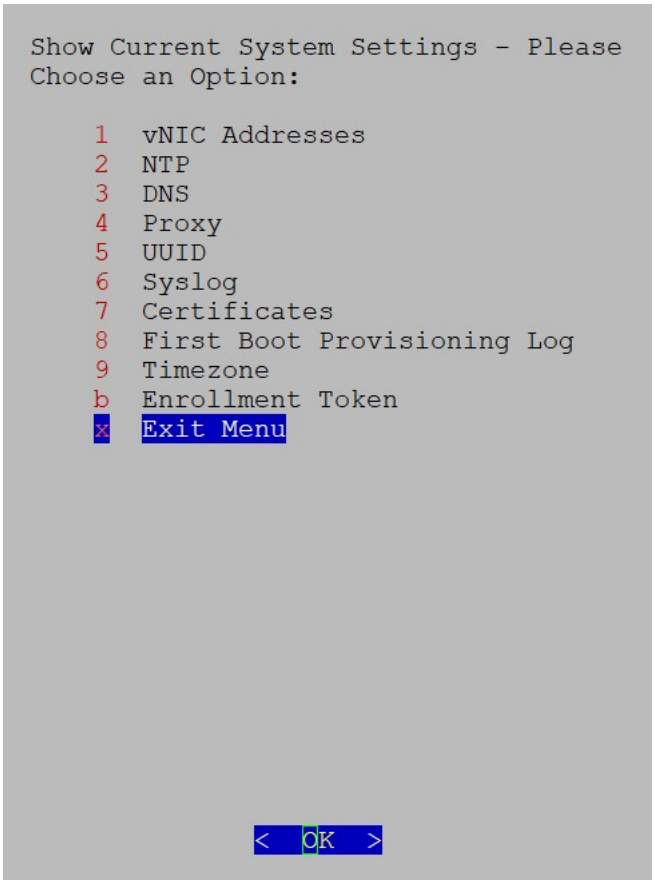
Step 2 Enter your current password and press **Enter**.

Step 3 Enter new password and press **Enter**. Re-type the new password and press **Enter**.

View Current System Settings

Crosswork Data Gateway allows you to view the following settings:

Figure 135: Show Current System Settings Menu



Follow these steps to view the current system settings:

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 you want to view.

Setting Option	Description
1 vNIC Addresses	Displays the vNIC configuration, including address information.
2 NTP	Displays currently configured NTP server details.
3 DNS	Displays DNS server details.
4 Proxy	Displays proxy server details (if any configured).
5 UUID	Displays the system UUID.

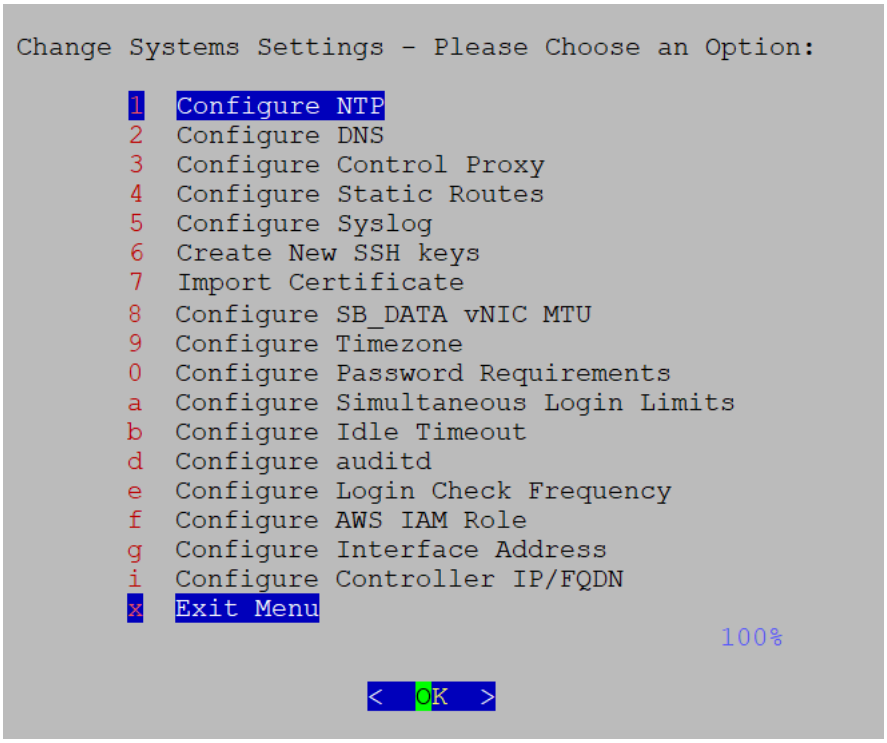
Setting Option	Description
6 Syslog	Displays the Syslog forwarding configuration. If no Syslog forwarding is configured, this will display only "# Forwarding configuration follows" on screen.
7 Certificates	Provides options to view the following certificate files: • Crosswork Data Gateway signing certificate file • Controller signing certificate file • Controller SSL/TLS certificate file • Syslog certificate file • Collector certificate file
8 First Boot Provisioning Log	Displays the content of the first boot log file.
9 Timezone	Displays the current timezone setting.
b Enrollment Token	**Attention** This menu option is for users of Crosswork Data Gateway for Cloud applications. Displays the token that Crosswork Data Gateway used to enroll with Crosswork Cloud.

Change Current System Settings

Crosswork Data Gateway allows you to configure the following settings:

Configure Crosswork Data Gateway Instance

Figure 136: Change System Settings Menu



Follow these steps to modify the current system settings:

Step 1 From the Main Menu, select **3 Change Current System Settings**.

Step 2 Select the setting that you want to modify.

- NTP
- DNS
- Control proxy
- Static routes
- Syslog
- SSH keys
- Certificate
- vNIC MTU
- Timezone
- Password requirements
- Simultaneous login limits
- Idle timeout
- Auditd

- Login check frequency
- *AWS IAM role
- Interface address
- Controller IP address
- *Enrollment token

Note
- In Crosswork versions earlier than 5.0, the Configure AWS IAM Role menu allowed updating the AWS IAM role in the AWS EC2 deployment. The AWS IAM role menu used during the configuration of southbound connections. This menu was specifically used when creating a High Availability (HA) pool.

  The 7.0 release no longer supports this menu and it is functionality is deprecated.
- The Enrollment token menu option is for users of Crosswork Data Gateway for Cloud applications.
- Crosswork Data Gateway system settings can only be configured by the administrator.
- When using an IPv6 address, it must be surrounded by square brackets ([1::1]).
- In the Settings options where you require to use SCP, if you are not using the default SCP port 22, you can specify the port as a part of the SCP command. For example,

  ```
  -P55 user@host:path/to/file
  ```

  Where 55 is a custom port.

Configure NTP

It is important that NTP time be synchronized with the controller application and its Crosswork Data Gateway instances. If not, then session handshake doesn't happen and functional images are not downloaded. In such cases, error message clock time not matched and sync failed is logged in controller-gateway.log. To access log files, see Run show-tech, on page 417. You can use Controller Reachability and NTP Reachability options from **Main Menu** > **Vitals** to check NTP reachability for the controller application as well as the Crosswork Data Gateway. See View Crosswork Data Gateway Vitals, on page 410. If NTP has been set incorrectly,you will see error Session not established.

When configuring Crosswork Data Gateway to use authentication via a keys file, the chrony.keys file must be formatted in a specific way as documented at https://chrony.tuxfamily.org/doc/3.5/chrony.conf.html#keyfile. For sites that use ntpd and are configured to use a ntp.keys file, it is possible to convert from ntp.keys to chrony.keys using the tool https://github.com/mlichvar/ntp2chrony/blob/master/ntp2chrony/ntp2chrony.py. The tool converts ntpd configuration into a chrony compatible format, but only the keys file is required to be imported into Crosswork Data Gateway.

Follow the steps to configure NTP settings:

Step 1 From the **Change Current System Settings** Menu, select **Configure NTP**.

Step 2 Enter the following details for the new NTP server:

- Server list, space delimited

- Use NTP authentication?
- Key list, space delimited and must match in number with server list
- Key file URI to SCP to the VM
- Key file passphrase to SCP to the VM

Step 3 Click **OK** to save the settings.

Configure DNS

Step 1 From the **Change Current System Settings** menu, select **Configure DNS** and click **OK**.
Step 2 Enter the new DNS server address(es) and domain.
Step 3 Click **OK** to save the settings.

Configure Control Proxy

If you have not configured a proxy server during installation, avail this option to set up a proxy sever:

Step 1 From the **Change Current System Settings** menu, select **Configure Control Proxy** and click **OK**.
Step 2 Click **Yes** for the following dialog if you wish to proceed. Click **cancel** otherwise.
Step 3 Enter the new Proxy server details:

- Server URL
- Bypass addresses
- Proxy username
- Proxy passphrase

Step 4 Click **OK** to save the settings.

Configure Static Routes

The static routes are configured when Crosswork Data Gateway receives add/delete requests from the collectors. The **Configure Static Routes** option from the main menu can be used for troubleshooting purpose.

Caution Static routes configured using this option are lost when the Crosswork Data Gateway reboots.

Add Static Routes

Follow the steps to add static routes:

Step 1 From the **Change Current System Settings** menu, select **4 Configure Static Routes**.
Step 2 To add a static route, select **a Add**.
Step 3 Select the interface for which you want to add a static route.
Step 4 Select the IP version.
Step 5 Enter IPv4 or IPv6 subnet in CIDR format when prompted.
Step 6 Click **OK** to save the settings.

Delete Static Routes

Follow the steps to delete a static route:

Step 1 From the **Change Current System Settings** Menu, select **4 Configure Static Routes**.
Step 2 To delete a static route, select **d Delete**.
Step 3 Select the interface for which you want to delete a static route.
Step 4 Select the IP version.
Step 5 Enter IPv4 or IPv6 subnet in CIDR format.
Step 6 Click **OK** to save the settings.

Configure Syslog

You can configure the remote servers during the Day0 installation through the configuration file. If you want to modify the Syslog server list, port number, protocol, and certificate file in Day1 installation or later use the Interactive Console.

Note For any Syslog server configuration with IPv4 or IPv6 support for different Linux distributions, please refer to your system administrator and configuration guides.

Follow the steps to configure Syslog:

Before you begin

Crosswork Data Gateway lets you configure multiple servers through the following modes:

- Simultaneous: Crosswork Data Gateway sends messages to all the configured Syslog server addresses. When one of the servers is unresponsive, the message is queued to the disk until the servers are response.
- Failover: Crosswork Data Gateway sends message to the first Syslog server address. If the server is not available, the message is sent to the subsequent configured address. When all the servers in the list are unresponsive, the message is queued to the disk until the servers are response.

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 **Simultaneous** or **Failover**.

Step 4 Enter the values for the following Syslog attributes:

- Server address or hostname: Space-delmited list of IPv4 or IPv6 address of Syslog server accessible from the management interface.
- Port: Port number of the Syslog server
- Protocol: Use UDP, TCP, or RELP when sending system logs.
- Use Syslog over TLS?: Use TLS to encrypt Syslog traffic.
- TLS Peer Name: Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.
- Syslog Root Certificate File URI: PEM formatted root cert of Syslog server retrieved using SCP.
- Syslog Certificate File Passphrase: Password of SCP user to retrieve Syslog certificate chain.

Step 5 Click **OK** to save the settings.

Create New SSH Keys

Creating new SSH keys will remove the current keys.

Follow the steps to create new SSH keys:

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 Certificate

Updating any certificate other than Controller Signing Certificate causes a collector restart.

Crosswork Data Gateway allows you to import the following certificates:

- Controller signing certificate file
- Controller SSL/TLS certificate file
- Syslog certificate file
- Proxy certificate file

Step 1 From the **Change Current System Settings** Menu, select **Import Certificate**.

Step 2 Select the certificate you want to import.

Step 3 Enter SCP URI for the selected certificate file.

Step 4 Enter passphrase for the SCP URI and click **OK**.

Configure vNIC2 MTU

You can change vNIC2 MTU only if you are using 3 NICs.

If your interface supports jumbo frames, the MTU value lies in the range of 60-9000, inclusive. For interfaces that do not support jumbo frames, the valid range is 60-1500, inclusive. Setting an invalid MTU causes Crosswork Data Gateway to revert the change back to the currently configured value. Please verify with your hardware documentation to confirm what the valid range is. An error will be logged into kern.log for MTU change errors which can be viewed after running showtech.

Step 1 From the **Change Current System Settings** menu, select **Configure vNIC1 MTU**.

Step 2 Enter the vNIC2 MTU value.

Step 3 Click **OK** to save the settings.

Configure Timezone of the Data Gateway VM

The data gateway VM first launches with default timezone as UTC. Update the timezone with your geographical area so that all the data gateway processes (including the showtech logs) reflect the timestamp corresponding to the location you have chosen.

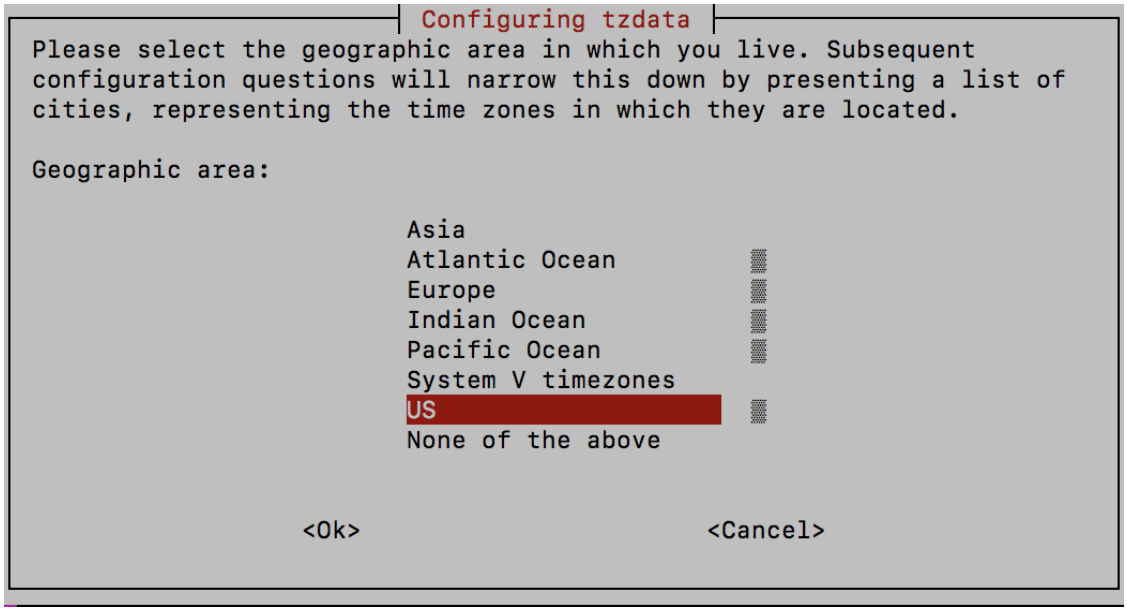
Step 1 Log in to the data gateway VM.

Step 2 In the data gateway VM interactive menu, select **3 Change Current System Settings**.

Step 3 From the menu, select **9 Timezone**.

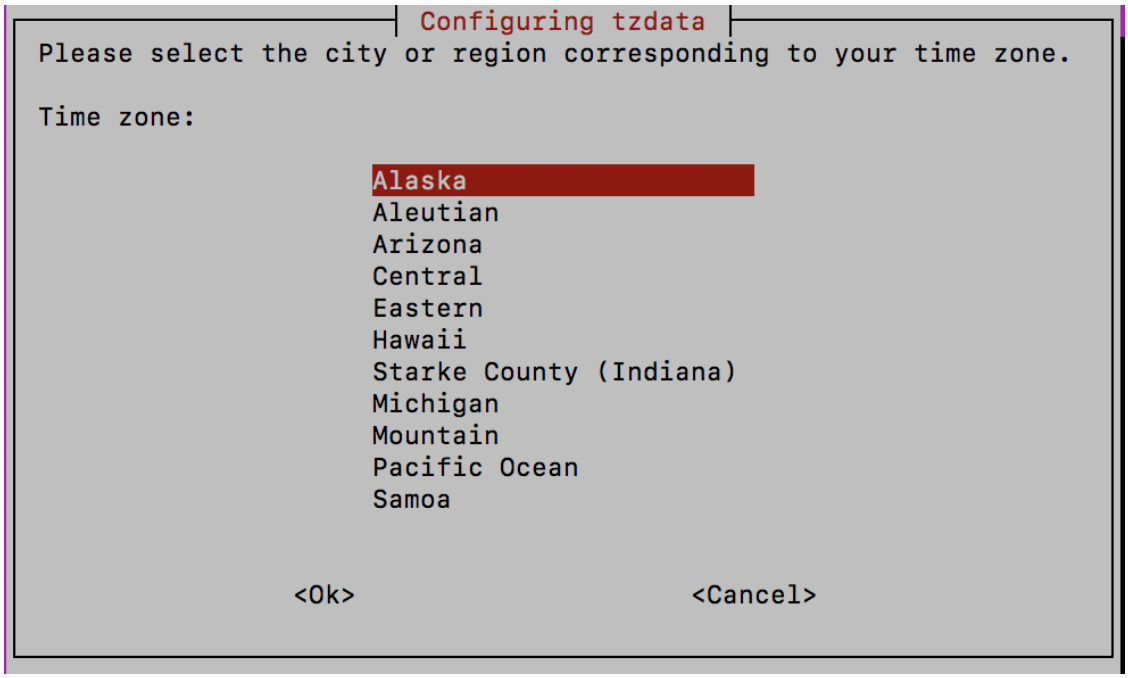
Step 4 Select the geographic area in which you live.

Figure 137: Timezone Settings - Geographic Area Selection



Step 5 Select the city or region corresponding to your timezone.

Figure 138: Timezone Settings - Region Selection



Step 6 Select **OK** to save the settings.

Step 7 Reboot the data gateway VM so that all processes pick up the new timezone. See *Reboot Crosswork Data Gateway VM* section in *Cisco Crosswork Network Controller 7.0 Administration Guide*.

Step 8 Log out of the data gateway VM.

Configure Password Requirements

You can configure the following password requirements:

- Password Strength
- Password History
- Password expiration
- Login Failures

Step 1 From **Change Current System Settings** menu, select **Configure Password Requirements**.

Step 2 Select the password requirement you want to change.

Set the options you want to change:

- **Password Strength**
  - Min Number of Classes
  - Min Length
  - Min Changed Characters
  - Max Digit Credit
  - Max Upper Case Letter Credit
  - Max Lower Case Letter Credit
  - Max Other Character Credit
  - Max Monotonic Sequence
  - Max Same Consecutive Characters
  - Max Same Class Consecutive Characters
- **Password History**
  - Change Retries
  - History Depth
- **Password expiration**
  - Min Days
  - Max Days
  - Warn Days
- **Login Failures**

- Login Failures
- Initial Block Time (sec)
- Address Cache Time (sec)

Step 3 Click **OK** to save the settings.

Configure Simultaneous Login Limits

By default, Crosswork Data Gateway supports 10 simultaneous sessions for the **dg-admin** and **dg-oper** user on each VM. To change this:

Step 1 From the **Change Current System Settings** menu, select **a Configure Simultaneous Login Limits**.
Step 2 In the window that appears, enter the number of simultaneous sessions for the **dg-admin** and **dg-oper** user.
Step 3 Select **Ok** to save your changes.

Configure Idle Timeout

Step 1 From the **Change Current System Settings** menu, select **b Configure Idle Timeout**.
Step 2 Enter the new value of idle timeout in the window that appears.
Step 3 Enter **Ok** to save your changes.

Configure Remote Auditd Server

Use this procedure to configure the auditd daemon export to a remote server.

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.

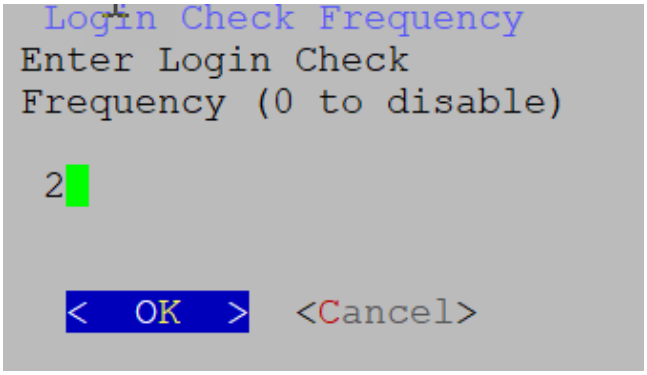
Configure Login Frequency

You can configure the number of permissible log in attempts the user can make after a log in failure.

Step 1 From the **Change Current System Settings** menu, select **Configure Login Check Frequency** and click **OK**.

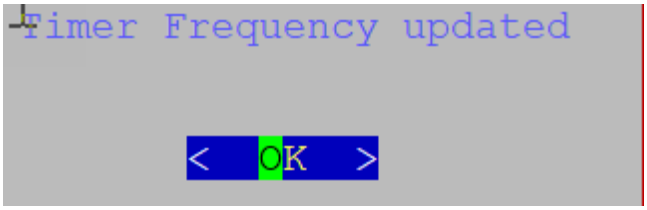
Step 2 In the **Login Check Frequency** window, enter the number of log in attempts you want to monitor. To disable the feature, enter 0.

Figure 139: Login Check Frequency Window



After the timer is updated, a confirmation window appears.

Figure 140: Timer Frequency Updated Window



Configure the Interface Address

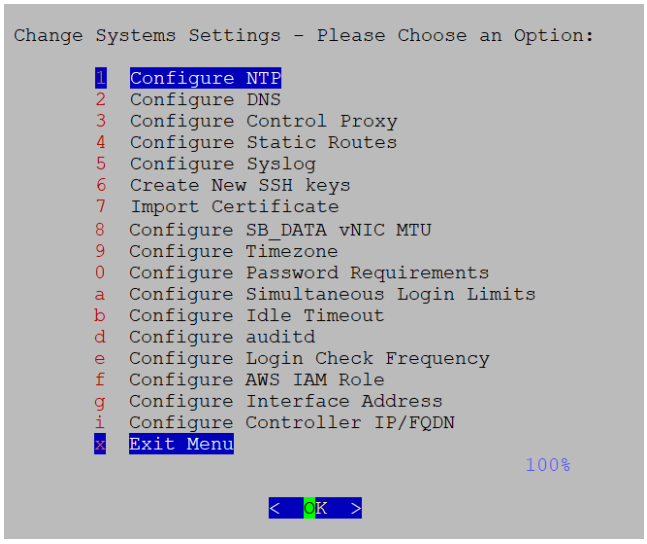
After you have deployed a Crosswork Data Gateway instance, you can reconfigure the interfaces that are already associated with an instance. When you reconfigure an interface, you can change its name, associate IP address, or access the security group that is associated with an interface.

Before you begin

- All the devices must be detached from the Crosswork Data Gateway instance for which you want to reconfigure the interface address.
- The Crosswork Data Gateway instance must be in the maintenance mode.

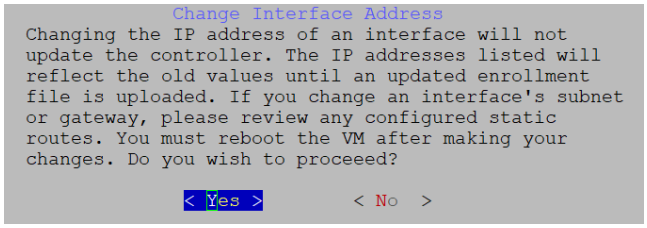
Step 1 From the **Change System Settings** menu, select **Configure Interface Address**.

Figure 141: Change System Settings Menu



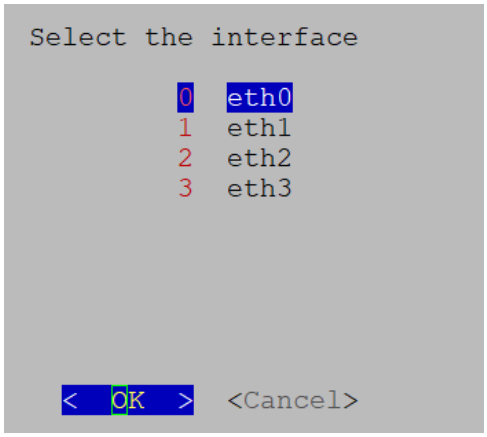
Step 2 In the **Change Interface Address** confirmation box, click **Yes**.

Figure 142: Change Interface Address Confirmation Message



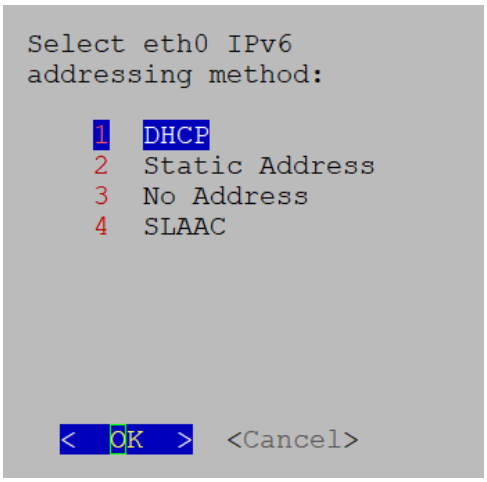
Step 3 Select the interface that you want to reconfigure and click **OK**. The options are `eth0`, `eth1`, `eth2`, or `eth3`.

Figure 143: Interface Selection Menu



Step 4 Select the <interface> IPv4 addressing method. The options are `DHCP`, `Static Address`, or `No address`. Cisco recommends that you select the option that you had specified during the Day0 installation.

Figure 144: IPv6 Address Selection



Step 5 Enter the IPv4 address and click **OK**.

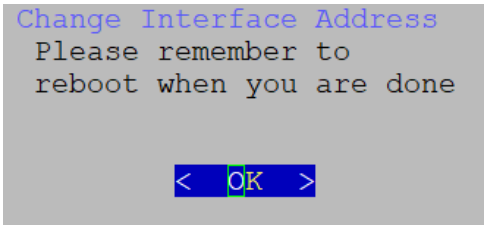
Step 6 Enter the IPv4 Netmask address and click **OK**.

Step 7 In the **Skip <interface> IPv4 gateway configuration confirmation** box, select `True` or `False` and click **OK**.

Step 8 If you have selected `True` in the previous step, specify the IPv4 gateway address.

Step 9 In the **Change Interface Address** confirmation box, click **OK**.

Figure 145: Confirmation Message



After the interface is configured, make sure to reboot the VM.

Configure Controller IP for Crosswork Data Gateway

This topic explains the procedure for configuring the Controller IP or 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 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.

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 controller IP.

A message appears to confirm that Crosswork has updated the controller's IP or FQDN, and the VM is rebooted.

The data gateway connects to Crosswork and progresses to the UP state. If the data gateways are in the Assigned state with devices attached, they resume data collection.

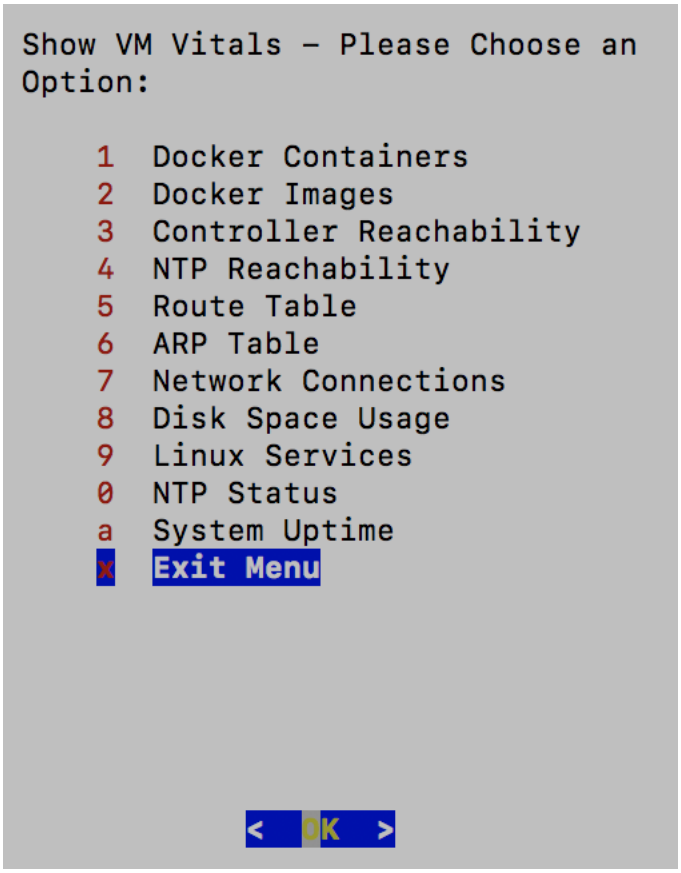
View Crosswork Data Gateway Vitals

Follow these steps to view Crosswork Data Gateway vitals:

Step 1 From the Main Menu, select **Vitals**.

Step 2 From the **Show VM Vitals** menu, select the vital you want to view.

Figure 146: Show VM Vitals Menu



Vital	Description
Docker Containers	Displays the following vitals for the Docker containers currently instantiated in the system: • Container ID • Image • Name • Command • Created Time • Status • Port
Docker Images	Displays the following details for the Docker images currently saved in the system: • Repository • Image ID • Created Time • Size • Tag
Controller Reachability	Displays the results of controller reachability test run: • Default IPv4 gateway • Default IPv6 gateway • DNS server • Controller • Controller session status
NTP Reachability	Displays the result of NTP reachability tests: • NTP server resolution • Ping • NTP Status • Current system time
Route Table	Displays IPv4 and IPv6 routing tables.
ARP Table	Displays ARP tables.
Network Connections	Displays the current network connections and listening ports.
Disk Space Usage	Displays the current disk space usage for all partitions.

Vital	Description
Linux Services	Displays the status of the following Linux services: • NTP • SSH • Syslog • Docker • Crosswork Data Gateway Infrastructure containers.
Check NTP Status	Displays the NTP server status.
Check System Uptime	Displays the system uptime.

Troubleshooting Crosswork Data Gateway VM

To access **Troubleshooting** menu, select **5 Troubleshooting** from the Main Menu.

Note The image shows the Troubleshooting menu corresponding to **dg-admin** user. Few of these options are not available to **dg-oper** user. See Table Table 55: Permissions Per Role, on page 393.

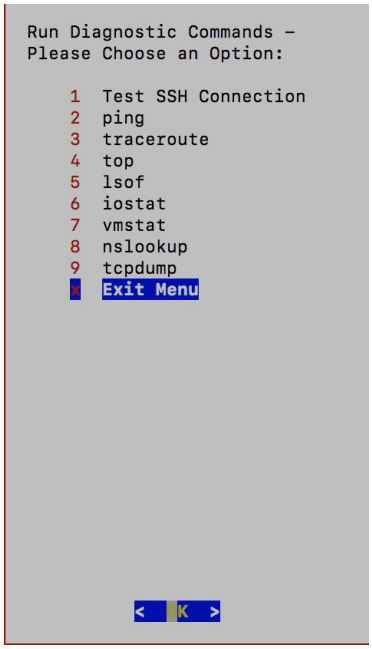
The **Troubleshooting** menu that provides the following options:

- Run Diagnostic Commands, on page 412
- Run show-tech, on page 417
- Reboot Crosswork Data Gateway VM, on page 417
- Shutdown the Crosswork Data Gateway VM, on page 418
- Export auditd Logs, on page 418
- Enable TAC Shell Access, on page 419

Run Diagnostic Commands

The **Run Diagnostics** menu provides you the following options in the console:

Figure 147: Run Diagnostics Menu



Ping a Host

Crosswork Data Gateway provides you ping utility that can be used to check reachability to any IP address.

Step 1 From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics** > **ping**.

Step 2 Enter the following information:

- Number of pings
- Destination hostname or IP
- Source port (UDP, TCP, TCP Connect)
- Destination port (UDP, TCP, TCP Connect)

Step 3 Click **OK**.

Traceroute to a Host

Crosswork Data Gateway provides the traceroute option to help troubleshoot latency issues. Using this option provides you a rough time estimate for the Crosswork Data Gateway to reach the destination.

Step 1 From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics** > **traceroute**.

Step 2 Enter the traceroute destination.

Step 3 Click **OK**.

Command Options to Troubleshoot

Crosswork Data Gateway provides several commands for troubleshooting.

Step 1 From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics**.

Step 2 Select the command and other option or filters for each of the commands:

- **4 top**
- **5 lsof**
- **6 iostat**
- **7 vmstat**
- **8 nsolookup**

Step 3 Click **Ok**.

Once you have selected all the options, Crosswork Data Gateway clears the screen and runs the command with the specified options.

Download tcpdump

Crosswork Data Gateway provides the tcpdump option that allows you to capture and analyze network traffic.

Note This task can only be performed by a **dg-admin** user.

Step 1 From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics** > **tcpdump**.

Step 2 Select an interface to run the tcpdump utility. To run the utility for all the interfaces, select the **All** option.

Step 3 Select the appropriate check box to view the packet information on the screen or save the captured packets to a file.

Step 4 Enter the following details and click **OK**.

- Packet count limit
- Collection time limit
- File size limit
- Filter expression

Depending on the option you choose, Crosswork Data Gateway displays the packet capture information on the screen or saves it to a file. After the tcpdump utility reaches the specified limit, Crosswork Data Gateway

compresses the file, and prompts for the SCP credentials to transfer the file to a remote host. The compressed file is deleted once the transfer is complete or if you've decided to cancel the file transfer before completion.

Run a Controller Session Test

After Crosswork Data Gateway is installed, you can validate if the instance is able to establish a connection with Crosswork Cloud by using the controller session test option. In addition to the connection tests, the utility validates and analyzes the discrepancies between the resources (CPU and memory) assigned to the VM and the resources prescribed by the deployment profile.

From Main Menu, navigate to **Troubleshooting** > **Run Diagnostics** > **Run Controller Session Tests**. If the connection is completed, the console displays a message indicating that the instance was able to establish a connection. When the connection fails, additional validation tests are performed, and the following information is displayed:

- DNS server IP address
- DNS domain
- NTP server address
- NTP status
- Proxy URL
- Proxy reachability status
- Controller URL
- Controller reachability status
- The date when the tests were last performed.

Configure Crosswork Data Gateway Instance

Figure 148: Run Controller Session Tests Menu

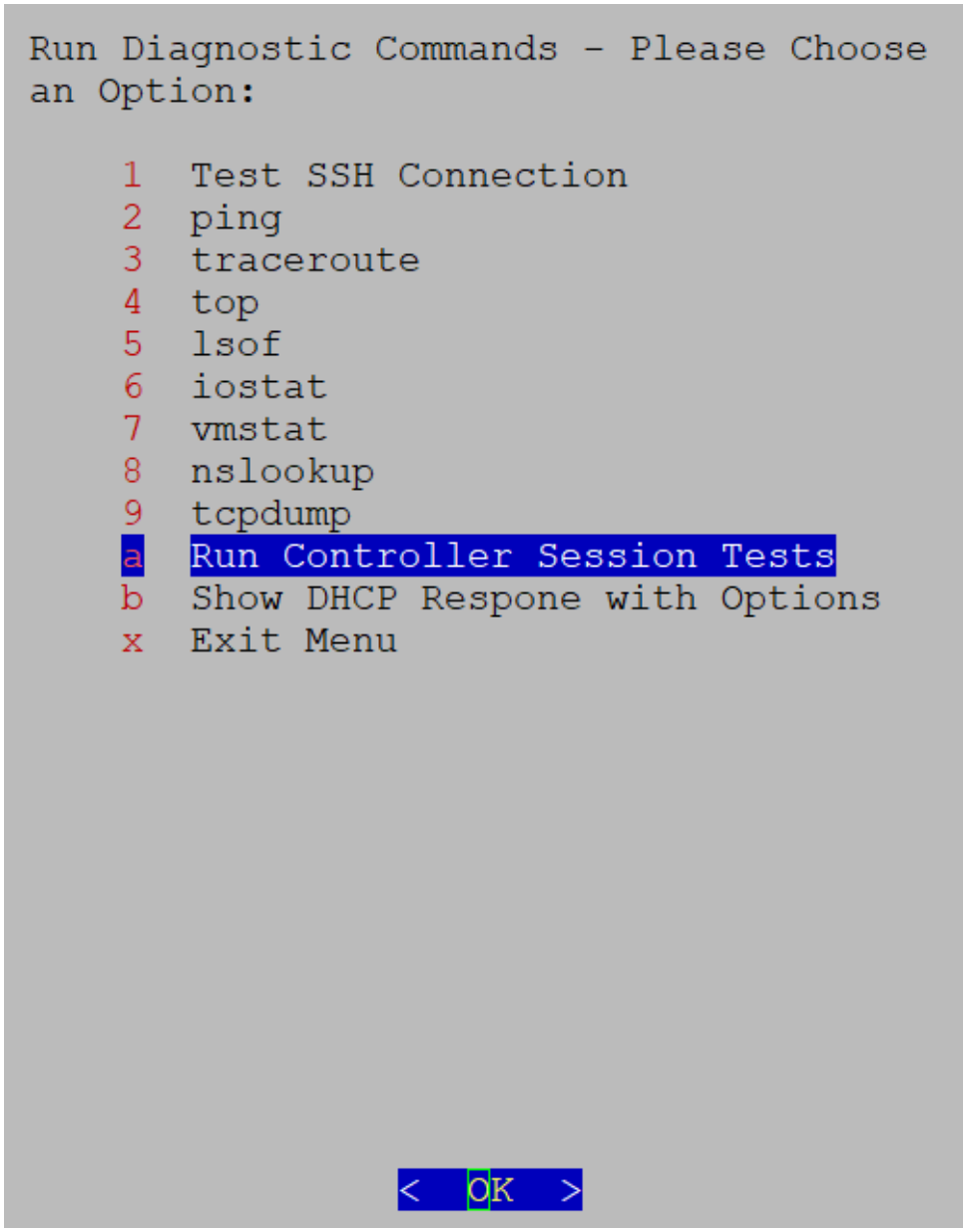
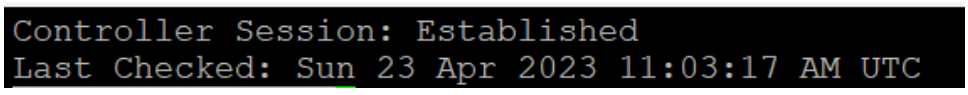


Figure 149: Result of the Run Controller Session Tests Menu



What to do next

If the controller session was not established, review the information displayed on the console to determine the probable cause of the failure and perform the corrective actions proposed on the console.

Run show-tech

Crosswork Data Gateway provides the show_tech option to export its log files to a user-defined SCP destination.

The collected data includes the following:

- Logs of all the Data Gateway components running on Docker containers
- VM Vitals

It creates a tarball in the directory where it is executed. The output is a tarball named `DG-<CDG version>-<CDG host name>-year-month-day--hour-minute-second.tar.xz.enc`.

The execution of this command may take several minutes depending on the state of Crosswork Data Gateway.

Step 1 From **Troubleshooting** menu, select **Show-tech** and click **OK**.

Step 2 Enter the destination to save the tarball containing logs and vitals.

Step 3 Enter your SCP passphrase and click **OK**.

The showtech file downloads in an encrypted format.

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

Step 4 After the download is complete run the following command to decrypt it:

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

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

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

Reboot Crosswork Data Gateway VM

Note This task can only be performed by **dg-admin** user.

Crosswork Data Gateway gives you two options to reboot the VM:

- **Remove all Collectors and Reboot VM**: Select this option from the **Troubleshooting** menu if you want to stop the containers that were downloaded after installation (collectors and offload), remove the images from docker, remove collector data and configuration and reboot VM. This returns the VM to a state just after initial configuration is complete with only infrastructure containers running.

- **Reboot VM**: Select this option from the **Troubleshooting** menu for a normal reboot.

Shutdown the Crosswork Data Gateway VM

From the **Troubleshooting** Menu, select **5 Shutdown VM** to power off the Crosswork Data Gateway VM.

Export auditd Logs

Follow the steps to export auditd logs:

Step 1 From **Troubleshooting**, select **Export audit Logs**.

Step 2 Enter a passphrase for auditd log tarball encryption.

Step 3 Click **OK**.

Re-enroll Crosswork Data Gateway

Follow the steps to re-enroll Crosswork Data Gateway:

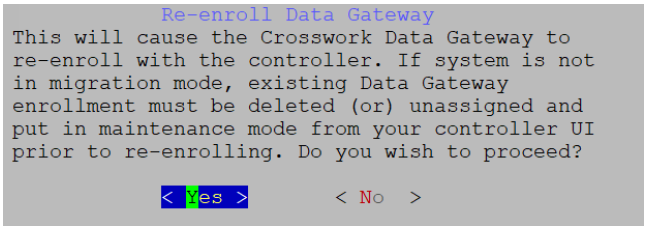
Before you begin

The existing Crosswork Data Gateway enrollment must be deleted from the controller prior to re-enrolling.

Step 1 From **Troubleshooting** menu, select **Re-enroll Data Gateway**.

Step 2 Review the information inn the confirmation window and click **Yes**.

Figure 150: Re-enroll Data Gateway Confirmation Window



Remove Rotated Log Files

Follow the steps to removes all rotated log files (*.gz or *.xz) in the `/var/log` and `/opt/dg/log` folders.

Step 1 From **Troubleshooting** menu, select **Remove Rotated Log files**.

Step 2 Select **Yes** in the dialog that appears to save your changes.

Enable TAC Shell Access

The TAC Shell Access function allows a Cisco engineer to directly log in to the Ubuntu shell via multifactor authentication, using a reserved user named **dg-tac**.

Initially, the **dg-tac** user account is locked and password is expired to prevent the user from getting a shell prompt. Once enabled, the dg-tac user is active until the next calendar day, 12:00 a.m UTC (midnight UTC), which is less than 24 hours.

The steps to enable the **dg-tac** user are as follows:

Note Enabling this access requires you to communicate actively with the Cisco engineer.

Before you begin

Ensure that the Cisco engineer who is working with you has access to the SWIMS Aberto tool.

Step 1 Log in to the Data Gateway VM as the **dg-admin** user.

Step 2 From the main menu, select **Troubleshooting**.

Step 3 From the **Troubleshooting** menu, select **t Enable TAC Shell Access**.

A dialog appears, warning that the **dg-tac** user login requires a password that you set and a response to a challenge token from TAC. At this point, you may answer **No** to stop the enable process or **Yes** to continue.

Step 4 If you continue, the system prompts for a new password to use and shows the day when the account disables itself.

Step 5 Enter a password to unlock the account in the console menu.

Step 6 Log out of the Crosswork Data Gateway.

Step 7 Follow these steps if the Crosswork Data Gateway VM can be accessed by the Cisco engineer directly. Move to **Step 8** otherwise.

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 Cisco engineer logs in as the **dg-tac** user Via SSH with the password you had set.

After entering the password, the system presents the challenge token. The Cisco engineer signs the challenge token using the SWIMS Aberto tool and pastes the signed response to the challenge token back at the Crosswork Data Gateway VM.

c) The Cisco engineer logs in successfully as the **dg-tac** user and completes the troubleshooting.

There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to 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 Crosswork Data Gateway VM cannot be accessed directly by the Cisco engineer, start a meeting with the Cisco engineer with desktop sharing enabled.

a) Log in as the **dg-tac** user Via SSH using the following command:

```
ssh dg-tac@<DG hostname or IP>
```

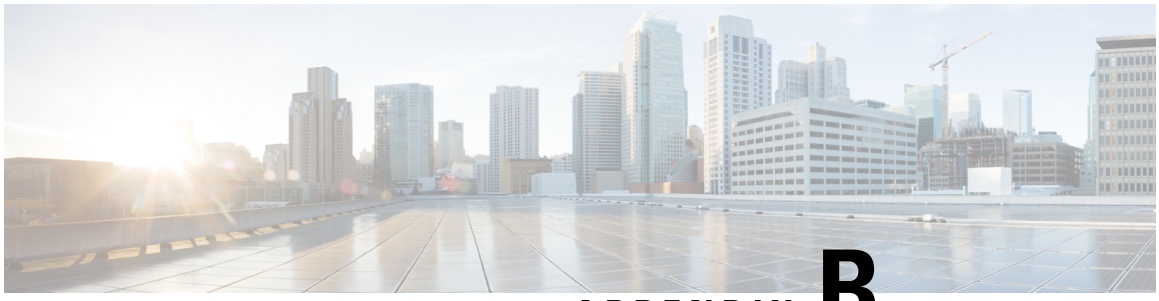
b) Enter the password that you set for the **dg-tac** user.

After entering the password, the system presents the challenge token. Share this token with the Cisco engineer who will then sign the token using the SWIMS Aberto tool and share the response with you.

c) Paste the signed response to the challenge token back to the Crosswork Data Gateway VM and press enter to get the shell prompt.
d) Share your desktop or follow the Cisco engineer's instructions for troubleshooting.

   There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to sign a new challenge to log in again.

e) Log out of the TAC shell after troubleshooting is complete.



APPENDIX B

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 is applicable only when Crosswork is the target application and is not limited when the target is an external application.

Note the following constraints:

- The system cannot extract index values from OIDs of conceptual tables. If any of the columns that define indices in the conceptual table are not populated, the index value is replaced 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 56: 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

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

List of Pre-loaded Traps and MIBs for SNMP Collection

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

List of Pre-loaded Traps and MIBs for SNMP Collection

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
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

List of Pre-loaded Traps and MIBs for SNMP Collection

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

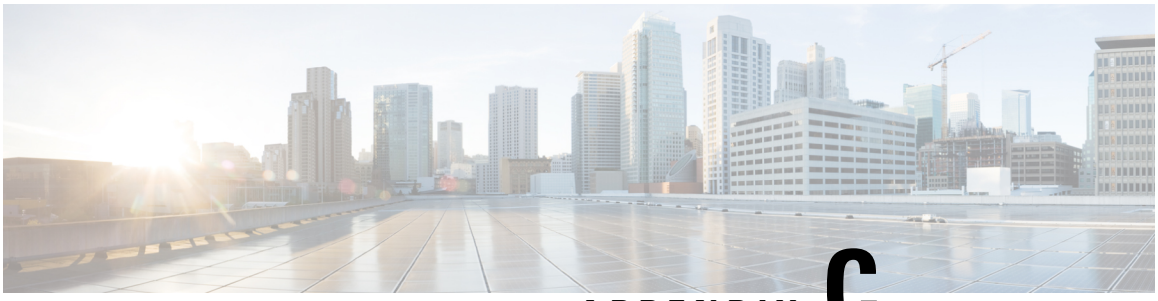
CISCO-IETF-IPMROUTE -MIB.mib	CISCO-UNIFIED-COMPUTING-NETWORK -MIB.mib	PPP-IP-NCP-MIB.mib
CISCO-IETF-ISIS -MIB.mib	CISCO-UNIFIED-COMPUTING-PROCESSOR -MIB.mib	PPP-LCP-MIB.mib
CISCO-IETF-MPLS-ID -STD-03-MIB.mib	CISCO-UNIFIED-COMPUTING-TC- MIB.mib	PPVPN-TC-MIB.mib
CISCO-IETF-MPLS-TE-EXT-STD-03- MIB.mib	CISCO-VLAN-IFTABLE-RELATIONSHIP -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
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

List of Pre-loaded Traps and MIBs for SNMP Collection

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 C

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.

cli_xr_bgp_oper.yang	Cisco-IOS-XR-ip-bfd-oper.yang
Cisco-IOS-XR-ipv4-bgp-oper.yang	Cisco-IOS-XR-asr9k-xbar-oper.yang
Cisco-IOS-XR-ipv4-acl-oper.yang	Cisco-IOS-XR-snmp-sensormib-oper.yang
Cisco-IOS-XR-shellutil-filesystem-oper.yang	Cisco-IOS-XR-config-cfgmgr-oper.yang
Cisco-IOS-XR-infra-alarm-logger-oper.yang	Cisco-IOS-XR-infra-fti-oper.yang
Cisco-IOS-XR-icpe-infra-oper.yang	Cisco-IOS-XR-dot1x-oper.yang
Cisco-IOS-XR-fretta-bcm-dpa-stats-oper.yang	Cisco-IOS-XR-sdr-invmgr-diag-oper.yang
Cisco-IOS-XR-cofo-infra-oper.yang	Cisco-IOS-XR-wanphy-ui-oper.yang
Cisco-IOS-XR-man-ems-oper.yang	Cisco-IOS-XR-bundlemgr-oper.yang
Cisco-IOS-XR-mpls-lsd-oper.yang	Cisco-IOS-XR-l2vpn-oper.yang
Cisco-IOS-XR-show-fpd-loc-ng-oper.yang	Cisco-IOS-XR-asr9k-qos-oper.yang
Cisco-IOS-XR-telemetry-model-driven-oper.yang	Cisco-IOS-XR-segment-routing-ms-oper.yang
Cisco-IOS-XR-shellutil-oper.yang	Cisco-IOS-XR-pfi-im-cmd-oper.yang
Cisco-IOS-XR-ip-iep-oper.yang	Cisco-IOS-XR-asic-errors-oper.yang
Cisco-IOS-XR-cdp-oper.yang	Cisco-IOS-XR-lib-keychain-oper.yang
Cisco-IOS-XR-ip-sbfd-oper.yang	Cisco-IOS-XR-sdr-invmgr-oper.yang
Cisco-IOS-XR-tty-management-cmd-oper.yang	Cisco-IOS-XR-ipv4-ospf-oper.yang
Cisco-IOS-XR-upgrade-fpd-oper.yang	Cisco-IOS-XR-pfm-oper.yang
Cisco-IOS-XR-crypto-macsec-secy-oper.yang	Cisco-IOS-XR-config-valid-ccv-oper.yang
Cisco-IOS-XR-ip-iarm-v6-oper.yang	Cisco-IOS-XR-ip-iarm-v4-oper.yang
Cisco-IOS-XR-ipv4-autorp-oper.yang	Cisco-IOS-XR-infra-statsd-oper.yang

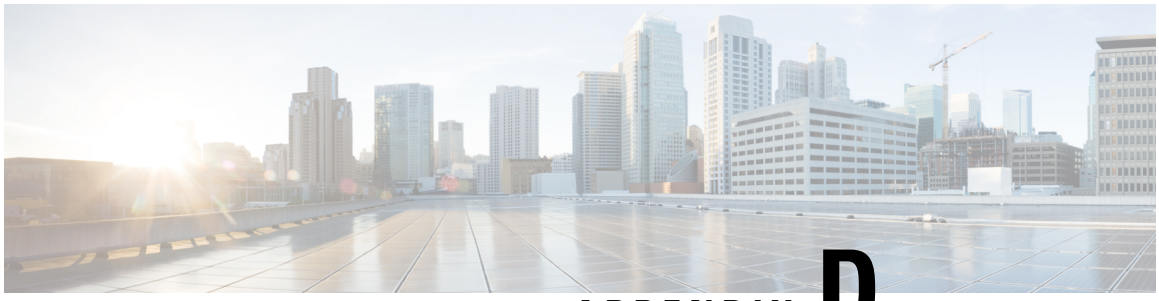
List of Pre-loaded YANG Modules for MDT Collection

Cisco-IOS-XR-pbr-vservice-ea-oper.yang	Cisco-IOS-XR-ipv4-vrrp-oper.yang
Cisco-IOS-XR-ip-domain-oper.yang	Cisco-IOS-XR-cmproxy-oper.yang
Cisco-IOS-XR-ipv4-io-oper.yang	Cisco-IOS-XR-crypto-ssh-oper.yang
Cisco-IOS-XR-ipv4-hsrp-oper.yang	Cisco-IOS-XR-controller-optics-oper.yang
Cisco-IOS-XR-freqsync-oper.yang	Cisco-IOS-XR-atm-vcm-oper.yang
Cisco-IOS-XR-aaa-diameter-oper.yang	Cisco-IOS-XR-dnx-driver-fabric-plane-oper.yang
Cisco-IOS-XR-ip-tcp-oper.yang	Cisco-IOS-XR-asr9k-lc-fca-oper.yang
Cisco-IOS-XR-drivers-media-eth-oper.yang	Cisco-IOS-XR-mpls-vpn-oper.yang
Cisco-IOS-XR-infra-policymgr-oper.yang	Cisco-IOS-XR-asr9k-sc-envmon-oper.yang
Cisco-IOS-XR-fretta-bcm-dpa-hw-resources-oper.yang	Cisco-IOS-XR-es-acl-oper.yang
Cisco-IOS-XR-subscriber-ipsub-oper.yang	Cisco-IOS-XR-evpn-oper.yang
Cisco-IOS-XR-infra-rsi-oper.yang	Cisco-IOS-XR-rptiming-tmg-oper.yang
Cisco-IOS-XR-prm-server-oper.yang	Cisco-IOS-XR-ethernet-lldp-oper.yang
Cisco-IOS-XR-l2rib-oper.yang	Cisco-IOS-XR-ip-ntp-oper.yang
Cisco-IOS-XR-subscriber-pppoe-ma-oper.yang	Cisco-IOS-XR-mediasvr-linux-oper.yang
Cisco-IOS-XR-ocni-local-routing-oper.yang	Cisco-IOS-XR-ipv6-ma-oper.yang
Cisco-IOS-XR-reboot-history-oper.yang	Cisco-IOS-XR-infra-rmf-oper.yang
Cisco-IOS-XR-asr9k-lpts-oper.yang	Cisco-IOS-XR-infra-correlator-oper.yang
Cisco-IOS-XR-infra-serg-oper.yang	Cisco-IOS-XR-mpls-static-oper.yang
Cisco-IOS-XR-rgmgr-oper.yang	Cisco-IOS-XR-snmp-entitymib-oper.yang
Cisco-IOS-XR-ncs1k-mxp-headless-oper.yang	Cisco-IOS-XR-pbr-vservice-mgr-oper.yang
Cisco-IOS-XR-aaa-nacm-oper.yang	Cisco-IOS-XR-pfi-im-cmd-ctrlr-oper.yang
Cisco-IOS-XR-infra-rcmd-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-resources-oper.yang
Cisco-IOS-XR-crypto-macsec-mka-oper.yang	Cisco-IOS-XR-macsec-ctrlr-oper.yang
Cisco-IOS-XR-tunnel-vpdn-oper.yang	Cisco-IOS-XR-ipv6-nd-oper.yang
Cisco-IOS-XR-ipv4-dhcpd-oper.yang	Cisco-IOS-XR-tunnel-l2tun-oper.yang
Cisco-IOS-XR-ip-rip-oper.yang	Cisco-IOS-XR-infra-dumper-exception-oper.yang
Cisco-IOS-XR-ncs1001-otdr-oper.yang	Cisco-IOS-XR-syncc-oper.yang
Cisco-IOS-XR-asr9k-asic-errors-oper.yang	Cisco-IOS-XR-dnx-driver-oper.yang
Cisco-IOS-XR-pmengine-oper.yang	Cisco-IOS-XR-ncs1k-macsec-ea-oper.yang
Cisco-IOS-XR-linux-os-reboot-history-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-drop-stats-oper.yang
Cisco-IOS-XR-ppp-ea-oper.yang	Cisco-IOS-XR-infra-sla-oper.yang
Cisco-IOS-XR-asr9k-ptp-pd-oper.yang	Cisco-IOS-XR-ncs1001-ots-oper.yang

Cisco-IOS-XR-ipv4-igmp-oper.yang	Cisco-IOS-XR-nto-misc-shmem-oper.yang
Cisco-IOS-XR-ipv4-bgp-oc-oper.yang	Cisco-IOS-XR-ip-rib-ipv4-oper.yang
Cisco-IOS-XR-ip-pfilter-oper.yang	Cisco-IOS-XR-ipv4-pim-oper.yang
Cisco-IOS-XR-lpts-pre-ifib-oper.yang	Cisco-IOS-XR-pppoe-ea-oper.yang
Cisco-IOS-XR-ipv6-ospfv3-oper.yang	Cisco-IOS-XR-infra-syslog-oper.yang
Cisco-IOS-XR-asr9k-netflow-oper.yang	Cisco-IOS-XR-crypto-sam-oper.yang
Cisco-IOS-XR-infra-xtc-oper.yang	Cisco-IOS-XR-Ethernet-SPAN-oper.yang
Cisco-IOS-XR-sysdb-oper.yang	Cisco-IOS-XR-lpts-ifib-oper.yang
Cisco-IOS-XR-lib-mpp-oper.yang	Cisco-IOS-XR-ethernet-link-oam-oper.yang
Cisco-IOS-XR-infra-xtc-agent-oper.yang	Cisco-IOS-XR-mpls-ldp-oper.yang
Cisco-IOS-XR-ip-rib-ipv6-oper.yang	Cisco-IOS-XR-tty-management-oper.yang
Cisco-IOS-XR-rptiming-dti-oper.yang	Cisco-IOS-XR-lmp-oper.yang
Cisco-IOS-XR-wd-oper.yang	Cisco-IOS-XR-nto-misc-shprocmem-oper.yang
Cisco-IOS-XR-man-xml-ttyagent-oper.yang	Cisco-IOS-XR-procmem-oper.yang
Cisco-IOS-XR-ip-daps-oper.yang	Cisco-IOS-XR-Subscriber-infra-subdb-oper.yang
Cisco-IOS-XR-spirit-install-instmgr-oper.yang	Cisco-IOS-XR-asr9k-np-oper.yang
Cisco-IOS-XR-fretta-grid-svr-oper.yang	Cisco-IOS-XR-ptp-oper.yang
Cisco-IOS-XR-clns-isis-oper.yang	Cisco-IOS-XR-tunnel-nve-oper.yang
Cisco-IOS-XR-ipv4-bgp-oper.yang	Cisco-IOS-XR-ocni-oper.yang
Cisco-IOS-XR-ipv4-ma-oper.yang	Cisco-IOS-XR-ncs6k-acl-oper.yang
Cisco-IOS-XR-l2-eth-infra-oper.yang	Cisco-IOS-XR-manageability-object-tracking-oper.yang
Cisco-IOS-XR-plat-chas-invmgr-oper.yang	Cisco-IOS-XR-ocni-intfbase-oper.yang
Cisco-IOS-XR-dwdm-ui-oper.yang	Cisco-IOS-XR-infra-tc-oper.yang
Cisco-IOS-XR-policy-repository-oper.yang	Cisco-IOS-XR-subscriber-session-mon-oper.yang
Cisco-IOS-XR-ipv6-new-dhcpv6d-oper.yang	Cisco-IOS-XR-ip-udp-oper.yang
Cisco-IOS-XR-subscriber-srg-oper.yang	Cisco-IOS-XR-ipv6-acl-oper.yang
Cisco-IOS-XR-manageability-perfmgmt-oper.yang	Cisco-IOS-XR-crypto-macsec-pl-oper.yang
Cisco-IOS-XR-dnx-port-mapper-oper.yang	Cisco-IOS-XR-aaa-tacacs-oper.yang
Cisco-IOS-XR-mpls-te-oper.yang	Cisco-IOS-XR-man-ipsla-oper.yang
Cisco-IOS-XR-nto-misc-oper.yang	Cisco-IOS-XR-invmgr-oper.yang
Cisco-IOS-XR-ppp-ma-oper.yang	Cisco-IOS-XR-ipv4-arp-oper.yang
Cisco-IOS-XR-config-cfgmgr-exec-oper.yang	Cisco-IOS-XR-aaa-locald-oper.yang
Cisco-IOS-XR-perf-meas-oper.yang	Cisco-IOS-XR-ha-eem-policy-oper.yang

List of Pre-loaded YANG Modules for MDT Collection

Cisco-IOS-XR-snmp-agent-oper.yang	Cisco-IOS-XR-ascii-ltrace-oper.yang
Cisco-IOS-XR-asr9k-lc-ethctrl-oper.yang	Cisco-IOS-XR-skp-qos-oper.yang
Cisco-IOS-XR-ifmgr-oper.yang	Cisco-IOS-XR-flowspec-oper.yang
Cisco-IOS-XR-iedge4710-oper.yang	Cisco-IOS-XR-icpe-sdacp-oper.yang
Cisco-IOS-XR-controller-otu-oper.yang	Cisco-IOS-XR-fretta-bcm-dpa-npu-stats-oper.yang
Cisco-IOS-XR-subscriber-accounting-oper.yang	Cisco-IOS-XR-alarmgr-server-oper.yang
Cisco-IOS-XR-ncs5500-qos-oper.yang	Cisco-IOS-XR-fia-internal-tcam-oper.yang
Cisco-IOS-XR-skywarp-netflow-oper.yang	Cisco-IOS-XR-tty-server-oper.yang
Cisco-IOS-XR-ncs1k-mxp-lldp-oper.yang	Cisco-IOS-XR-qos-ma-oper.yang
Cisco-IOS-XR-fib-common-oper.yang	Cisco-IOS-XR-aaa-protocol-radius-oper.yang
Cisco-IOS-XR-dnx-netflow-oper.yang	Cisco-IOS-XR-platform-pifib-oper.yang
Cisco-IOS-XR-lpts-pa-oper.yang	Cisco-IOS-XR-asr9k-fsi-oper.yang
Cisco-IOS-XR-ncs1k-mxp-oper.yang	Cisco-IOS-XR-ncs5500-coherent-node-oper.yang
Cisco-IOS-XR-asr9k-sc-invmgr-oper.yang	Cisco-IOS-XR-snmp-ifmib-oper.yang
Cisco-IOS-XR-ptp-pd-oper.yang	Cisco-IOS-XR-ip-mobileip-oper.yang
Cisco-IOS-XR-ethernet-cfm-oper.yang	Cisco-IOS-XR-wdsysmon-fd-oper.yang
Cisco-IOS-XR-pbr-oper.yang	Cisco-IOS-XR-infra-objmgr-oper.yang
Cisco-IOS-XR-ip-rsvp-oper.yang	Cisco-IOS-XR-ipv6-io-oper.yang
Cisco-IOS-XR-terminal-device-oper.yang	Cisco-IOS-XR-plat-chas-invmgr-ng-oper.yang
Cisco-IOS-XR-mpls-oam-oper.yang	Cisco-IOS-XR-ncs5500-coherent-portmode-oper.yang
Cisco-IOS-XR-sse-span-oper.yang	Cisco-IOS-XR-infra-dumper-oper.yang
Cisco-IOS-XR-asr9k-sc-diag-oper.yang	Cisco-IOS-XR-mpls-io-oper.yang



APPENDIX D

Cisco EPM Notification MIB

This section contains the following topics:

Cisco EPM Notification MIB

The following table shows the mapping of event fields to the alarm model in CISCO-EPM-NOTIFICATION-MIB.

Note Some of the values in the following table may appear truncated in a PDF. Please refer to the HTML version for clarity.

Table 57: Cisco-EPM-Notification-MIB

Event Field	Snmpvarbind	OID	Description	Example
TimeStamp	cenAlarmTimestamp	1.3.6.1.4.1.9.9.311.1.1.2.1.3	The time when the event was raised	1639759929
AlarmId	cenAlarmInstanceID	1.3.6.1.4.1.9.9.311.1.1.2.1.5	The unique alarm instance ID	57e3ef70-1597
Type	cenAlarmType	1.3.6.1.4.1.9.9.311.1.1.2.1.8	Type of Event	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*	3

Event Field	Snmpvarbind	OID	Description	Example
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 String is formatted in '<integer, eventCategory description>	3, System
	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) 1:ipv4, 2:ipv6	1:ipv4
	cenAlarmServerAddress	1.3.6.1.4.9.9.311.1.1.2.1.12	The IP Address of the CW alarm centre (VIP)	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	DLM
Description	cenAlarmDescription	1.3.6.1.4.9.9.311.1.1.2.1.16	A detailed description of the event	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	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 is formatted in '<integer, eventSeverity description>'	3,Major

Event Field	Snmpvarbind	OID	Description	Example
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 is formatted in '<ObjectDescription=xx, ObjectId=xx>'	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	0
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	9f19e5a9-a64c

Cisco EPM Notification MIB